

~~SECRET~~

OGC 77-3636

7 June 1977

MEMORANDUM FOR: Director of Central Intelligence

FROM : 25X1
General Counsel

SUBJECT : PRM/NSC-11 Subcommittee Reports to the SCC

1. Action Requested. None. The several attachments, none of which unfortunately makes very light reading, are for your information.

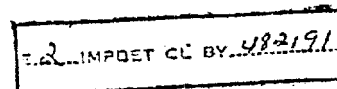
2. Background: As you know, PRM/NSC-11 established a subcommittee under the direction of the Attorney General, known popularly as the Part I subcommittee (the reference being to the operative paragraph in PRM/NSC-11), to review the adequacy of various existing laws relating to intelligence activities. This subcommittee has been chaired by John Harmon, Assistant Attorney General, Office of Legal Counsel, and I have served as your representative. State, DOD, OMB and the NSC were separately represented. The first subcommittee product was the draft legislation dealing with electronic surveillance carried out within the United States for the purpose of gathering foreign intelligence or counterintelligence. This legislation, the Foreign Intelligence Surveillance Act of 1977, was considered at a SCC meeting on 14 April, attended by both you and me, and it has been introduced in the Congress and will shortly be the subject of hearings both before the Senate Judiciary Committee and the SSCI. The remaining fruits of the subcommittee labors are attached. They are all in the form of reports to the SCC and presumably will be considered at one or more SCC meetings yet to be scheduled. The reports deal with, respectively:

(a) Intelligence Charter Legislation (Tab A)

This report recommends that another subcommittee be formed, to include representatives of all SCC members (this could be accomplished simply by perpetuating the Part I subcommittee and giving it a new assignment), to take on the job of drafting intelligence agency charter legislation. The SSCI head start in this charter-drafting enterprise is cited as a reason for the urgency of this recommendation. Once the proposed subcommittee is established, the report envisions (as does the memorandum from the Secretary of Defense to

NOTE COMINT ATTACHMENT F

~~SECRET~~



to Dr. Brzezinski dated 26 May 1977) that its initial efforts will be directed to the so-called "abuse" questions (electronic surveillance abroad, unconsented physical searches, clandestine collection and covert action, etc.), with the structural and organizational questions, characterized as more complex, left for second-stage consideration. The idea would be to have the whole package together by 30 September and in the interim to negotiate with the SSCI about each separate piece as drafts are made ready and approved by the SSC. [Brown's memorandum to Brzezinski, by contrast, suggests a deadline of 6-8 weeks, which I regard as totally unrealistic, for the drafting of legislation on the "abuse" questions, with no deadline specified as to the structural and organizational questions.] John Harmon understands that you oppose any deferral of the community organization issues and that you will be pressing for prompt resolution of those issues.

(b) Unauthorized Disclosure of Sensitive Information (Tab B)

25X1 This report deals with the problem of leaks of national security information. Its recommendations are essentially negative, except for a proposal that another hard look be taken at E.O. 11652, which is the basic directive governing the classification system. [The latter proposal requires no action by the SCC since a thoroughgoing review of E.O. 11652, to be completed by 15 September, has already been mandated by PRM/NSC-29 dated 1 June 1977. Per your decision of 18 May, [] of this Office will serve as your representative on the review committee, which will be chaired jointly by as yet unappointed members of the NSC and Domestic Council staffs.]

25X1 There is a CIA dissent to this report, which I wrote and forwarded to you for information on 2 June. The point of the dissent has to do with the way in which the report defines the problem. As I see it, except in special situations, leaks are not punishable under existing law - that is, for example, if Messrs. Boyce and Lee had given the [] documents to the press instead of the Soviets, in my view there would not have been any prosecution, nor even any legally supportable basis for any prosecution, apart possibly from a charge of theft. The report, on the other hand, takes the position that existing statutory authorities are by and large adequate, and that the real problem is that, for various reasons, particularly intelligence agency refusals to agree in advance to declassify the materials needed for use as evidence in prosecution, there is no vigorous program of enforcement.

(c) The Freedom of Information and Privacy Acts (Tab C)

This report does not recommend a push for legislation to add some new exemption to the FOIA or to otherwise broadly amend the statute. We initially had urged the subcommittee to recommend that legislation be sought exempting certain intelligence agency files from FOIA review and disclosure requirements, on grounds that the heavy administrative burdens imposed by the statute are not justified in

~~SECRET~~

~~SECRET~~

public benefit terms, given the small amount of information that is ultimately released. But the case we made on this score was unpersuasive, and the prospect of favorable action in the Congress would be poor even if our case were much better than it is, so in the end we gave up the chase.

This report does put forward one more modest proposal, namely that an effort be made to obtain legislation amending the FOIA to restrict the rights that it confers to U. S. citizens and permanent resident aliens, that is, to exclude foreigners from the class of eligible requesters.

(d) Executive Order 11905 (Tab D)

This report recommends a set of revisions, largely of a housekeeping variety, in E.O. 11905. It does not address Section 3 of the order (Control and Direction of National Intelligence Organizations) or any of the substantive questions concerning the structure of the intelligence community. Rather it concerns itself in the main with the clarification of provisions of the Order that have proven to be confusing, ambiguous or unworkable, and with the correction of inadvertent errors of omission or commission that were made when the Order was originally drafted early in 1976. Among other things, it is proposed that the role of the DEA in the intelligence community be recognized (see pages 43-45).

The bulk of the report (pages 18-43) is devoted to consideration of a single controversial issue - whether and how far there should be a revision of Section 4(a)(5) of E.O. 11905, which requires senior officials of the intelligence community to report to the Attorney General "that information which relates to detection or prevention of possible violations of law by any person, including an employee of the senior official's department or agency." The dispute does not revolve around mandatory reporting of official abuses or possible law violations by intelligence agency employees, which all agencies regard as a proper requirement and which in any event is covered by separate statute, 28 U.S.C. 535(b), applicable to all executive departments and agencies. Rather the dispute centers on the language of Section 4(a)(5) that obligates senior intelligence officials, alone among all executive branch officials, to report possible law violations by all persons, including persons having no connection with the conduct of intelligence.

We have favored the elimination of Section 4(a)(5), the effect of which would be to put intelligence agency obligations back on a par with the obligations that apply elsewhere within the executive branch. This option is discussed on pages 21-28. The Justice Department favors retention of Section 4(a)(5), modified however so as to narrow its scope by enumerating those particular

~~SECRET~~

possible offenses that would remain subject to a reporting obligation. This option is discussed on pages 29-39, and other possible options are discussed on pages 39-43. Our position is rational but probably unacceptable from a political standpoint. My guess is that the Justice Department's compromise position, which would represent a significant improvement if adopted, represents the best bargain that is practical and attainable under the present circumstances.

(e) Lack of Authority for Electronic Surveillance Abroad and Physical Searches Within and Without the United States (TAB E-1)

This report proposes stop-gap measures, pending the enactment of legislation (see item (a) above), in the area of electronic surveillance and unconsented physical searches. These measures would take the form of a delegation from the President authorizing the Attorney General to approve electronic surveillance conducted by the CIA against U.S. persons abroad, as well as certain unconsented physical searches conducted in the United States, or conducted abroad and directed against U.S. persons, on the condition however that no such unconsented physical searches are to involve break-ins or non-consensual entries. These measures are made necessary, at least in the eyes of the Attorney General, by the asserted absence of any outstanding delegation of authority by the President that would permit Attorney General approval of the activities in question.

It is my view that the Attorney General already has the authority to approve the activities in question, as evidenced by the existing electronic surveillance and unconsented physical search procedures (see item (f) below) implementing Sections 5(b)(2) and 5(b)(3) of E. O. 11905. Assuming the need for a further grant of authority from the President, however, the proposed delegation, while limited, is probably adequate. — Only occasionally we will ever want to engage in the activities the delegation does authorize the Attorney General to approve (in CIA's case, electronic surveillance or unconsented physical searches directed against a U.S. person abroad reasonably believed to be an agent of a foreign power), and it is very unlikely that we would ever want to engage in the activities the delegation does not authorize the Attorney General to approve (breaking and entering to conduct an unconsented physical search).

*/ In my written comments on an earlier draft of this report, attached at Tab E-2, see pages 3-4, I suggested certain additions to the proposed delegation, intended to clarify its applicability and the Attorney General's authority in the area of international terrorism. These changes were not made. However, I am informed by the responsible attorneys in the Office of Legal Counsel that their failure to include my suggested additional language does not reflect a disagreement but only their conclusion that the necessary authority is already implicit in the proposed delegation as drafted.

~~SECRET~~

(f) Attorney General Procedures (Tab F)

This report discusses a number of problems that have arisen in regard to the Attorney General procedures, issued during the last administration, governing the interception of electronic communications by CIA and NSA (not limited to SIGINT operations but including CIA audio and teltap operations as well).

As the overall scheme is accurately summarized on page 2 of the report, the procedures in general operate

(1) to require the prior approval of the Attorney General before any United States person may be targeted, which approval can be granted only if the United States person is an agent of a foreign power, - (2) to require the destruction of all intercepted communications which have a United States person as a party unless the communication contains significant foreign intelligence or other information specified in the procedures, and (3) to require the deletion of the identity of any United States person reflected in an intercepted communication, even if he was not a party to the communication, unless certain strict criteria are met.

For the most part, these restrictions are said by the Justice Department to reflect legal requirements from which there is no escape. In some part, however, DOJ views the restrictions not as dictates of the law but rather as expressions of policy. It is with respect to the restrictions that fall in this latter category, especially those that inhibit intelligence agency support of federal law enforcement in the area of international narcotics trafficking, that the debate is most heated, witness the discussion on pages 21-41 of the report.

As noted above, the Attorney General procedures require the destruction of intercepted communications having a U.S. person participant, and the deletion of the identity of any U.S. person who may be mentioned in an intercepted communication, even though he himself is not a party to the communication,

* The definition of United States person in these procedures is quite broad, including any person for whom a warrant would be required if the electronic surveillance were for other than foreign intelligence purposes. Here too, the Attorney General's procedures extend further than the mandate of Section 5(b)(2), E.O. 11905.

unless the communication constitutes significant foreign intelligence or one of the several other criteria is met. As matters now stand, it is not enough to justify retention or dissemination that the communication contains information concerning international narcotics trafficking, and as a consequence this sort of information gets screened out and is lost to the enforcement agencies that might put it to use.

Not surprisingly the enforcement agencies object to these restrictions, the loudest complaints coming from DEA. CIA and NSA on the other hand are content with the restrictions, since they tend to minimize the risk of involvement in the law enforcement process and therefore to avoid pressures (discovery demands, etc.) that can lead to a compromise of sources or operations. DOJ believes that the CIA and NSA concerns are overstated but is otherwise neutral in the debate. Its position is that these particular restrictions are not legally required and can readily be lifted should the SCC prefer that course.

This is a complicated business, but you should be aware that the CIA/NSA stance is politically dangerous (because it leaves us open to a charge that we are not supporting DEA and the federal narcotics control effort to the extent we are legally free to do so), and that in my judgment our stance warrants rethinking on its merits. I say that, however, without a true appreciation of the impacts, as for example on DDO or NSA record-keeping systems, that might be produced if these particular restrictions were to be relaxed or lifted.

You should also be aware that this report contains a very expansive statement on intelligence agency authority to "participate" in law enforcement activities (see pages 26-28). Assuming it is ratified by the SCC, that statement will not be an unmixed blessing by any means, since we can expect urgings from the law enforcement community, with DEA probably again in the forefront, to "participate" to the fullest extent of our authority.

3. There is a lot in the attached reports to chew on, and this memorandum is nothing more than an overview. I am certain you will want more detailed briefings before the SCC meets to consider these reports.

25X1

Attachments

~~SECRET~~

Original - DCI w/att

1 - DDCI w/att

1 - ER w/o att

25X1

1 - A/DDCI/

1 - DDO w/att

1 - DDA w/att

1 - DDS&T w/att

1 - DDI w/att

1 - OLC w/att

BEST COPY
Available

Intelligence Charter Legislation: Procedures

EXECUTIVE SUMMARY

The attached memorandum is a recommendation by the PRM-11 Subcommittee to the SCC for two procedures for dealing with intelligence charter legislation:

1. Coordinating Subcommittee. It is recommended that the President designate a subcommittee consisting of representatives of all SCC members. The subcommittee would serve as a working group to coordinate the drafting and negotiating of charter legislation.

2. Initial Issues. To begin to make progress on those pieces of charter legislation which respond to the abuses of the past while deferring the more complex question about the structure of the Intelligence Community, the following issues should be addressed first by the subcommittee in its dealings with the Congress:

a) Search and Surveillance (Electronic surveillance of Americans abroad; procedures for physical search.)

b) Restrictions on Clandestine Collection and Covert Action

c) Domestic Security Investigations (FBI investigation of domestic terrorism.)

DRAFT

SENATE SUBCOMMITTEE: RECOMMENDATION TO THE JOINT

Intelligence Charter Legislation: Procedures

I. Introduction

In his meeting with the Senate Select Committee on Intelligence on May 13, the President expressed his commitment to work with Congress to obtain legislation establishing the authority and responsibility of the intelligence agencies and the structure within which intelligence activity is conducted. He stated that he favored general charters, which would not unduly restrict the flexibility of the executive branch in administering intelligence activities.

The President also informed the Committee that he would not use an Executive order to preempt the passage of charter legislation. He requested that Congress refrain from introducing charter bills before the executive branch has had an opportunity to finish its intelligence review and to formulate specific policies on the various components of charter legislation. The Committee leaders indicated that they wanted to work in close cooperation with the executive branch and that they would not rush the introduction of charter legislation, although no firm timetable was established.

The Committee has nearly completed at least an initial draft of most major provisions of charter legislation. The Committee is pressing to begin work with representatives of the Administration on the details of

these drafts and to introduce legislation at the earliest opportunity. Thus, there is a need to move rapidly to organize a mechanism within the executive branch to begin to draft charters and deal with the Congress with respect to the drafts that have already been produced.

II. Coordinating Subcommittee

It is the recommendation of the PRT-II Subcommittee that the President should designate a coordinating subcommittee for charter legislation similar to the group which has coordinated the drafting and negotiating of the foreign intelligence surveillance bill. It would include representatives of the members of the SCC: the Director of Central Intelligence and the Intelligence Community staff, the Department of Defense, the Department of State, the Department of Justice, the National Security Council staff, and the Office of Management and Budget. Representatives of affected intelligence agencies such as NSA and the FBI would participate by arrangement with their respective departments.

The subcommittee would make recommendations to the SCC on the major policy questions involved in the drafting of charter legislation. The subcommittee would draft legislation consistent with the decisions of the SCC. Where a component of the charter legislation relates primarily to the activities of one agency, that agency would submit drafts to the subcommittee to ensure that there is consistency of form and coherence of policy in the Administration's charter package.

After the subcommittee has agreed upon a draft of a piece of the charter legislation, representatives of the subcommittee would enter detailed discussions of the proposed drafts with congressional staff.

III. Initial Issues

Because charters will raise such a wide range of issues to be resolved within the executive branch and because the Senate Committee has a significant headstart in the drafting process, it is recommended that the SCC select a limited set of initial issues for consideration by the proposed subcommittee. Three points should be kept in mind in selecting the initial issues:

(1) Timing. The SCC must digest a complex, difficult set of options before the subcommittee will be able to draft legislation dealing with the structure of the Intelligence Community. The resolution of the general questions of structure and organization are likely to require a longer period for deliberation than many other issues which could be dealt with separately. If other issues are chosen as starting points for the subcommittee, they must be substantial enough so that the Senate Intelligence Committee understands that a good faith effort is being made to begin the process and that structural questions will not be ignored.

(2) Abuse Questions. The discussion with Congress about the structure of the Intelligence Community is apt to be clouded and confused by the related attempt to design procedures for controlling abuses. Unless the

aura of abuse can be dissipated before the beginning of detailed discussions with Congress about questions of structure and organization, any structural proposal by the executive branch might be viewed with suspicion as a means of avoiding rigorous procedures to control abuse. Thus, it is recommended that the Administration move first to draft and negotiate with Congress in several legislative areas which will safeguard against abuse. This will establish a sense of good faith so that the more complex structural questions can then be discussed dispassionately.

(3) Political Context. The Inouye Committee has organized its charter efforts into two Subcommittees--Senator Ruddleston's Subcommittee on Charters and Guidelines and Senator Bayh's Subcommittee on the Rights of Americans. Because both Subcommittees have substantial drafts that are ready for consideration and because both Subcommittee chairmen believe that it is politically important to show progress on charters, it is advisable for the Administration to select initial issues that relate to the work of each Subcommittee.

In light of these factors, it is recommended that the SCC direct the proposed subcommittee to begin the drafting and negotiation process with the following issues:

A. Foreign Intelligence (Ruddleston Subcommittee)

Initial Issue:

- Restrictions on Clandestine Collection and Covert Action.

(The Buddleston draft charter sections include topics such as: restrictions on payments to clergy and others; dissemination of propaganda within the U.S.; paramilitary activities; assassinations; support of foreign police forces.)

Subsequent Issues:

- Role and Powers of the Director of Central Intelligence. (Structure of Intelligence Community; budget mechanisms; and communications security policy.)
- Foreign Counterintelligence (Authorization and restriction of techniques; review and policy mechanisms.)
- Oversight (Internal review; reporting to the Intelligence Oversight Board; reporting to Congress.)

B. Rights of Americans (Bayh Subcommittee)

Initial Issues:

- Search and Surveillance. (The Administration is already committed to drafting a separate bill to extend safeguards to Americans abroad with respect to overseas electronic surveillance. Senator Bayh is planning to raise this issue when his Subcommittee holds hearings on the foreign intelligence surveillance bill. Legislation is also needed to clarify the authorization and restrictions for the technique of physical search of the property and premises of foreign intelligence and counterintelligence targets both in the U.S. and abroad.)

- Domestic Security Investigations (Both the Attorney General and several Senate Committees have recently raised the question of the legal authority for the FBI to conduct preventive investigations of domestic political groups suspected of terrorist activity. Legislation in this area is urgently needed.)

Subsequent Issues:

- Foreign Intelligence Affecting the Rights of Americans (Clandestine collection about Americans working for foreign powers; economic intelligence about U.S. firms; CIA recruitment within the U.S.)

- Domestic Counterintelligence (Restrictions and authorization for counterintelligence within the U.S.)

- Minimization Procedures (The Bayh Subcommittee has expressed interest in considering the questions of maintenance, use, and dissemination of information in a general manner, rather than writing separate procedures for each agency.)

- Security/Background Investigations of Agency Employees.

IV. Agency Charters and Timetable

While the subcommittee is placing priority on the initial issues for drafting and negotiating which are indicated above, each intelligence agency should proceed to draft a separate charter on those issues which are unique to the agency.

At its first meeting, the subcommittee should establish a timetable for the drafting of the components of a charter package so that the entire package can be completed by September 30.

June 1, 1977 h

Subcommittee Report to the SCC
Executive Summary

Re: Unauthorized Disclosure of Sensitive Information

The attached report to the SCC is made pursuant to PRM/NSC-11 by the subcommittee acting under the direction of the Attorney General.

The report addresses the problem of unauthorized disclosure of classified information. Because this problem relates directly to the classification system itself, the report concludes that a thorough review of that system is a necessary first step to any resolution of the problem of leaks. In addition, the report notes that the existing criminal laws barring the unauthorized disclosure of certain specific kinds of classified information have not been enforced over several Administrations because of the various political and security costs involved in investigating and prosecuting leaks.

The subcommittee concludes that the same policy reasons which have precluded the investigation and prosecution of leaks in the past are still relevant and that the price for passage of legislation generally criminalizing the unauthorized disclosure of classified information is a price too high to pay for the marginal utility of such legislation.*/*

Other means of addressing the problem of unauthorized disclosures are also discussed, e.g., reducing access, Secrecy Agreements, disciplinary measures, civil actions, increased use of polygraphs, and the conclusion is that no feasible option is likely to have more than the most marginal impact on leaks, while each option has significant negative costs.**/*

/ The CIA dissents from this conclusion. Its conclusion and the reasons therefor are attached as Appendix 1.

**/* The Department of Defense takes exception to the thrust of the subcommittee's report on Secrecy Agreements and in addition wishes to emphasize the importance of investigating leaks even if prosecution is not the desired end. The Department of Defense's views are attached as Appendix 2.

May 31, 1977

REPORT TO THE SCC PURSUANT TO PRM/NSC-11

Re: Unauthorized Disclosure of Sensitive Information

Leaks of sensitive information have plagued the Government for a number of years, and in recent years as a result of a growing distrust of the Executive and investigations of intelligence agencies such leaks have been relatively more numerous.^{*/} There has been a consistent sense of frustration on the part of the Executive at the apparent inability to take effective action against leaks.

The information leaked in just the past several years has included military secrets, foreign policy secrets, and intelligence secrets--the latter two being the most sensational. Ordinarily such information is classified pursuant to E. O. 11652, which requires a determination at the minimum that information to be classified, if disclosed without authorization, "could reasonably be expected to cause damage to the national security." This is the basic Executive-wide standard for determining which information is to be protected against

^{*/}"Leaks," for purposes of this report, refer both to anonymous leaks to the press and to attributed publications by persons who previously had access to classified information.

unauthorized disclosure, and the application of certain criminal statutes turn on whether information is so classified. See 18 U.S.C. § 798, 50 U.S.C. § 783(b) & (c). As such, the Order as written and the practice under it cannot be separated from the problem of leaks.

E.O. 11652 was issued in 1972 in an attempt to correct the problems perceived in E.O. 10501, as amended, which had been the basis for the classification system. The perceived problems included rampant overclassification, the lack of an effective downgrading and declassification process, and too widespread authority to classify information. E.O. 11652, therefore, significantly restricted the number of persons who could originally classify information Secret or Top Secret, created schedules for review and declassification of information exempted from automatic downgrading and declassification, prohibited overclassification and unnecessary classification, prohibited classification to conceal inefficiency, administrative error, or to prevent embarrassment to a person or department, and created the Interagency Classification Review Committee (ICRC) to "review and take action to ensure compliance" with the Order. Nevertheless, the same problems remain today as before E.O. 11652, with little significant

change. That is, while the number of persons with original classification authority for Top Secret and Secret has been cut, although the number is still large, any employee may by "derivative authority" classify documents.*/ The exemptions from the General Declassification Schedule are overused, and information so exempt need only be reviewed after 10 years, and then only upon a request for review. And finally, the prohibition against overclassification has simply been ineffective, and it may be fairly said that the greatest abuses have been at the highest levels of Government, either through outright overclassification or because information overclassified at lower levels is not, when it comes to the attention of higher authorities, promptly sent back for downgrading or declassification.

The result of these continuing problems is a cynical attitude toward classified information by many in the Executive Branch, Congress, and the public. This cynical attitude is reinforced when classified information is deliberately disclosed by responsible officials, yet the

*/ If information is extracted from a classified document, it must be "derivatively" classified. For example, PRM/NSC-11 is classified Secret, but because it does not indicate what information therein is and is not classified, even the letters and numbers "PRM/NSC-11," should be classified Secret whenever referred to in another document. This obviously leads to unnecessary classification.

information remains classified, e.g., PD/NSC-2 was classified Confidential, but its entire substance was briefed to the press by the White House Press Office immediately upon its issuance.*/ While it is difficult to assess the extent to which this cynical attitude is responsible for leaks, there are certain leaks which may be fairly confidently attributed to this attitude, e.g., many of the leaks originating from the House Intelligence Committee. Perhaps more important, the cynical attitude toward classified information in Congress, where repeated statements assert that 99% of classified information need not be classified, makes any new statute either rationalizing the existing criminal penalties in the manner of S. 1 or extending prohibitions, as President Ford's suggested bill would have done, most difficult, if not impossible, to pass.

The subcommittee recommends that a thorough review of E.O. 11652 be made for the purpose of again attempting

*/ The widespread and blatant disregard for various provisions of the Executive Order, e.g., Section 4(A), condoned by the silence of high authorities, if not evidenced by them, further engenders a disrespect for the Executive Order generally and raises questions about attempts to maintain a strict standard as to other provisions, i.e., prohibitions against unauthorized disclosure.

to devise systemic safeguards against overclassification, but the subcommittee recognizes that no systemic changes, absent Draconian measures, can ever substantially alleviate the problem of overclassification absent a strong and continuous commitment by those high in Government to scrutinize closely everything they classify and everything which comes to their attention under their delegations to insure that information is not classified or exempted from general downgrading and declassification unless the information clearly warrants it.

The subcommittee also suggests that substantial consideration be given to placing the oversight role, as the ICRC and the NSC have under E.O. 11652, in an independent body such as the IOB, which would not reflect the institutional biases that inevitably result when the proverbial foxes are guarding the hen house.

Notwithstanding the limitations of E.O. 11652, it cannot be doubted that the majority of leaks would have occurred whether or not the classification system itself was perfect. And there is general agreement that the Executive Branch's actions to combat leaks has been ineffectual. Indeed, in the majority of cases no action

at all has been taken, either preventive or investigative.*/
In many cases the lack of action was a deliberate decision by those involved; in some the lack of action occurred for lack of a decision.

To understand the reasons why a conscious decision not to investigate was made, and to assess the validity of such decisions, it is necessary to describe the limitations of current law, self-imposed Executive Branch limitations, and the costs of investigating and taking action against leakers.

It has often been pointed out that there exists no law which generally prohibits the unauthorized disclosure of classified information. The statutes which specifically refer to classified information, 18 U.S.C. § 798 and 50 U.S.C. § 783, respectively prohibit the unauthorized disclosure of classified communications intelligence information and the unauthorized communication of classified information to an agent of a foreign government or a

*/ For purposes of the Report the formation of the "Plumbers" Group and its activities, wrongheaded in its conception and largely illegal in execution, are considered the equivalent of "no action," because it was the perceived inability to take other effective action which led to the formation of the "Plumbers."

member of a "Communist organization."*/ The Espionage Act, 18 U.S.C. § 793(d) & (e), prohibits the communication of "information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation" to a person not authorized to receive it. While the term "national defense" has been broadly construed to mean "a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness," Gorin v. United States, 312 U.S. 19, 28 (1941), it is doubtful whether the term even so construed includes all foreign relations matters and intelligence matters. For instance, it would be difficult to characterize the information in the Washington Post article dealing with payments to King Hussein as information relating to the national defense. Thus, many leaks have occurred which do not seem to fall within the proscription of any criminal statute. **/

*/ 42 U.S.C. § 2277 carries a \$2,500 criminal fine for the unauthorized disclosure of atomic energy information which is "classified" pursuant to the statutory classification system for such information, see 42 U.S.C. § 2161 et seq.

**/ The current bill to revise the criminal code will not affect any of these statutes.

Even where a leak might be covered by a criminal statute, prosecution may be inadvisable. First, all of the above statutes require at the minimum that the information disclosed be entered into evidence^{*/} and that the prosecution prove either that it was classified or that it was in fact national defense information. To do this requires declassification of the information and confirms the accuracy of the information disclosed.^{**/} In addition, in prosecutions under 18 U.S.C. § 793(d) or (e), it is necessary for the Government to prove that the leaker could reasonably believe that the information could harm the United States or aid a foreign nation. On the one hand, this can be exceptionally difficult to prove, especially where no apparent harm or aid has resulted from the leak (this was the case in the Ellsberg trial). Effective proof on this point may require further

^{*/} This much is probably constitutionally required.

^{**/} Because at one time the FBI routinely investigated leaks only to be informed after the expenditure of manpower and resources that the affected agency would not declassify the necessary information for prosecution, the FBI has now for several years required agencies requesting investigations of leaks to complete a form which in effect amounts to an agreement to declassify the necessary information for prosecution. Between 1965 and 1973 at least fourteen suspected leaks were not investigated or prosecuted because the affected agency would not declassify the necessary information.

disclosure of classified information--either the harm or aid which has resulted or other classified information to demonstrate how in context the information disclosed could harm the United States or aid a foreign nation.

Because of the inadequate coverage of existing laws and the difficulties involved in prosecutions under them, the Executive Branch has attempted without success since at least 1957 to obtain new legislation which would generally criminalize the unauthorized disclosure of classified information. A law providing criminal penalties for the unauthorized disclosure of classified information by a Government employee would close a loophole that exists in the law less through conscious decision than through inadvertence. It would be consistent with other laws which punish the unauthorized disclosure of information by Government employees, see 5 U.S.C. § 552a(i)(1) (information disclosed in violation of the Privacy Act); 18 U.S.C. § 1902 (disclosure of crop information); 18 U.S.C. § 1905 (disclosure of trade secrets or financial information required to be reported to the Government); 18 U.S.C. § 1906 (disclosure of names of borrowers or collateral for loans by a bank examiner).

The subcommittee, however, has concluded that the costs of passage of such legislation if it could be passed at all, probably outweigh the marginal utility such legislation would have, at least at the present time. The subcommittee is of the view that until the Executive Branch has effectively utilized the laws and mechanisms now available to it to prevent and investigate leaks, no new legislation should be sought.

This conclusion is based on the fact that in the past even where an effective statute was available, e.g., 18 U.S.C. § 793, no investigative or prosecutorial action has been taken. The reasons for this lack of action are likely to continue even if a law generally prohibiting the unauthorized disclosure of classified information were enacted.

There are several reasons why the Executive has failed to take action on leaks in the past. First, an investigation may give added publicity to the leaked information or confirm its accuracy, thereby compounding the problem. Second, as the Daniel Ellsberg case illustrates, prosecutions against leakers may have an adverse, rebound effect because of a perception that the Government is

trying to cover-up wrongdoing or impropriety. This perception is reinforced if the leak involves allegations of misconduct or wrongdoing. Third, leaks are often traced to Congressional committees; investigations of members of Congress or their staffs carry high political costs. Fourth, leaks are often made to newsmen who are either protected from forced disclosure of their sources or are prepared to stand in contempt rather than do so. Fifth, the Department of Justice has consistently refused to undertake criminal investigations unless the affected agency agrees to declassify by time of trial the information necessary to obtain a conviction, and intelligence agencies have generally refused to make such an agreement. Sixth, in some cases the affected intelligence agency has acted unilaterally or in concert with the intelligence service of another government in such a way as to taint any possible case against the individual. Seventh, there has been a wide-spread notion that leaks would gradually dry up as investigations of, and the consequent interest in, intelligence agencies' activities came to an end. Eighth, there has been some skepticism whether investigative efforts within lawful boundaries would be able to determine the source of leaks, the concern being that an unproductive investigation would demonstrate the Government's impotence.

Because these considerations cut across institutional lines, in the past neither the White House, the affected intelligence agencies, nor the Department of Justice has been willing to push for investigation. Therefore, unless and until all affected agencies jointly decide that the price for investigation and vigorous prosecution is a price worth paying to counter leaks, no additional legislation will have more than the most marginal effectiveness. Moreover, as the Executive has demonstrated that it is unwilling to investigate and prosecute leaks under a criminal statute already on the books, 18 U.S.C. § 798, there is little basis for the Executive to request legislation prohibiting leaks of classified information in other areas.

It has been suggested that civil penalties could be utilized to punish leaks. Civil penalties could be of two sorts--(1) civil fines or (2) disciplinary action against current Executive Branch officers and employees. The first would require legislation. In addition, where the leaker was unknown many of the factors weighing against investigation would remain, and some of the tools available to investigate criminal offenses--e.g., the grand jury--would

be unavailable. In the trial it would still be necessary to introduce into evidence the classified material leaked, thereby confirming the accuracy of the leak. Moreover, it would be difficult to determine the scale of a civil fine that would provide an adequate deterrence to those who stand to make substantial sums by publishing their memoirs. Finally, it would present an anomaly for disclosure of crop information to carry a criminal penalty, see 18 U.S.C. § 1902, but disclosure of national security secrets to carry a civil penalty.

The second option--disciplinary action against employees--would not require new legislation. Such disciplinary action could range from removal of a security clearance to suspension and discharge of the employee, see 5 U.S.C. § 7532. While in most cases the employee would be entitled to a hearing prior to discharge, it might be possible to avoid disclosure of classified information in the hearing consistent with the employee's due process and statutory rights.^{*/} This possibility alone makes this an attractive option.

This option could, of course, only be utilized against current members of the Executive Branch, and thus is limited.

^{*/}—Prior to or concurrent with an initiation of a program to investigate and take disciplinary measures against employees, a full review and probable rewriting of regulations regarding such disciplinary actions will be required to assure that they comport with statutory and constitutional requirements.

Moreover, investigations to determine the identity of a leaker will again be frustrated by the inability to compel cooperation or testimony. The FBI is of the view that in the overwhelming majority of cases the leaker will not be able to be found pursuant to such an investigation. Finally, investigations for civil or disciplinary purposes suffer some of the same costs as criminal investigations, e.g., giving added publicity to the leak or confirming its accuracy, creating the impression of a cover-up, and, if the investigation is unsuccessful, demonstrating the impotence of the Government.

It has been suggested that the use of polygraphs could aid in such non-criminal investigations. The validity of polygraphs has always been a subject of some doubt, but the real utility of polygraphs is not in their ability to distinguish ultimately between truth and falsehood, but in their ability to intimidate persons into telling the truth--either initially because they believe a lie will be caught or after a lie, because the examiner reveals there has been an indication of a lie and asks the question again, giving the person the opportunity to change his response. In a non-criminal investigation a polygraph examination could only be

Moreover, investigations to determine the identity of a leaker will again be frustrated by the inability to compel cooperation or testimony. The FBI is of the view that in the overwhelming majority of cases the leaker will not be able to be found pursuant to such an investigation. Finally, investigations for civil or disciplinary purposes suffer some of the same costs as criminal investigations, e.g., giving added publicity to the leak or confirming its accuracy, creating the impression of a cover-up, and, if the investigation is unsuccessful, demonstrating the impotence of the Government.

It has been suggested that the use of polygraphs could aid in such non-criminal investigations. The validity of polygraphs has always been a subject of some doubt, but the real utility of polygraphs is not in their ability to distinguish ultimately between truth and falsehood, but in their ability to intimidate persons into telling the truth--either initially because they believe a lie will be caught or after a lie, because the examiner reveals there has been an indication of a lie and asks the question again, giving the person the opportunity to change his response. In a non-criminal investigation a polygraph examination could only be

administered with consent, and traditional policy has been that refusal to undergo an examination results in no action against or inference of guilt toward the refuser.*/ Moreover, a polygraph can never be more than an adjunct to other investigative tools--the cost of using polygraphs would be excessive unless its use is restricted to situations in which the field of potential suspects had been narrowed to a rather small number.

It is current FBI practice to use polygraphs in security cases (including leaks) where it is deemed worthwhile, and therefore unless their use is intended to be substantially expanded, no change in policy is required.

It has also been suggested that further restricting access to classified information could help alleviate the problem of leaks. This could be effected in several ways, e.g., reducing the number of persons with security clearances, with the highest security clearances, or with codeword clearances; tightening the requirements for access to classified information even among persons who

*/ While consent to undergo a polygraph exam probably could be made a condition of employment in sensitive positions or to hold security clearances, such a requirement raises other questions, see infra.

have the proper clearance; increasing compartmentation by creation of new codewords.

Under E.O. 11652 before any person is allowed access to classified information he must have been determined to be trustworthy and his access to the information must be necessary for the performance of his duties. A security clearance is nothing more than the determination that a person is trustworthy. The fact that one has a security clearance should not mean that he has or should have access to any particular classified information. As a practical matter, however, the possession of the requisite security clearance is often considered sufficient grounds for giving someone classified information. Therefore, cutting the number of security clearances in the Government is likely to result in a certain diminution of unnecessary dissemination of classified information.

The question of a need-to-know as a requisite to access to classified information is often confused with the granting of a security clearance, and some departments and agencies do not grant specific clearances until a need-to-know has been established. The Subcommittee suggests that the review of E.O. 11652 should include consideration of changing the grounds for obtaining a security clearance, to require both a determination of trustworthiness and a need to work with classified information.

In addition, the Defense Department has had success with periodic reviews of the need for persons to have security clearances--in the sense that the reviews have resulted in substantial numbers of security clearances being removed as no longer necessary. The subcommittee recommends that the review of E.O. 11652 should consider a requirement of periodic reviews of the continuing necessity of existing security clearances.

It must be recognized, however, that elimination of unnecessary security clearances will likely bring only marginal results because those persons with unnecessary clearances normally do not in fact continue to have access.

And, further restricting access by a means other than reducing the number of unnecessary clearances would be of even less utility. Executive Order 11652 already restricts access to those who have a need-to-know, and access to certain compartmented information is on a "must know" basis. These standards should be enforced--and generally are--but it would seem that access to classified information within the Executive Branch cannot be further restricted without concurrently eliminating the newly established control and review mechanisms.

It is also questionable to what extent additional restrictions on access would be effective in stemming leaks. The persons from the Executive Branch who have been identified with publicized leaks of classified information (i.e., Ellsberg, Agee, Marchetti, Smith, Kahn) would have had justified access even under stricter standards. Moreover, with respect to untraced leaks apparently emanating from the Executive Branch, indications are that the persons responsible are small in number and rather well placed. In short, restrictions on access within acceptable limits are not likely to solve the problem.

While it might be useful to limit the number of Congressmen who are currently briefed on covert activities pursuant to the Hughes Amendment, 22 U.S.C. § 2422, and while the Executive Branch should encourage appropriate Congressional action, even if successful it is unlikely that such a limitation will meaningfully reduce the number of leaks.

Finally, the idea of creating more categories of compartmented information is criticized widely throughout the Intelligence Community, which is already questioning the cost-benefit relationship in the current compartmentations.

The use of polygraphs as a condition of access to certain information or to hold certain positions has been suggested. Polygraph tests now are required of applicants for employment at CIA and NSA, with follow-up polygraph examinations in the course of their careers. Consent to these examinations is a condition of both initial and continued employment. This procedure has never suffered any legal challenge or significant public disapprobation. While it cannot be demonstrated that these polygraph examinations have deterred leaks, it is reasonable to conclude that persons wishing continued employment would be deterred from leaking if subjected to periodic polygraph examinations.

Nevertheless, any meaningful expansion of polygraph examinations is likely to be met with criticism, and no feasible expansion could hope to cover all possible sources of leaks within the Executive Branch. Many of the personnel who fill the positions or have the access which would be covered by an expansion of the examinations are not career employees, and the threat of periodic examinations may not be meaningful to them because they expect to finish their Government service before they are examined again. Finally, certain agencies have expressed a loathing for polygraph

examinations under such circumstances, and it is likely that many individuals because of their position or prestige would feel insulted to be subjected to such an examination, and absent the most explicit Presidential direction, it would be impossible to enforce the requirement against such individuals.

It has also been suggested that the courts be used to enjoin the publication of classified information. There are severe problems, however, in obtaining such injunctions. Legally, there is some doubt whether with or without a specific statute authorizing such injunctions a court may ever enjoin the publication of information protected by the First Amendment. Nevertheless, under existing case law, it would appear that there are two situations in which an injunction against the publication of classified information might be obtained. The first is when the publication necessarily would result in substantial, direct, immediate, and irreparable damage to this Nation. See New York Times Co. v. United States, 403 U.S. 713 (1971) (Opinions of Brennan, Stewart, Burger, Harlan, and Blackmun). Obviously, it would take an extraordinary disclosure to meet this test, and this injunctive power is therefore of little benefit except in grave emergencies.

The other situation is where an injunction may be obtained to enforce a contract. This was the situation in United States v. Marchetti, 466 F.2d 1309 (4th Cir.), cert. denied, 409 U.S. 1063 (1972), where the United States obtained an injunction against the publication of certain sections of a book by a former CIA employee. The contract involved in that case was a secrecy agreement made by Marchetti in consideration for his employment with CIA. The success of the Government in the Marchetti case was quite limited in that substantial amounts of sensitive, classified information were allowed to be published. Moreover, injunctive relief premised upon secrecy agreements cannot hope to limit meaningfully the unauthorized disclosure of classified information, because it is the rare situation where the Government will have the prior knowledge of a disclosure necessary to obtain an injunction.

In E.O. 11905 the President required all employees of the Executive Branch and its contractors given access to information containing sources and methods of intelligence, as a condition of obtaining access, to undertake a Secrecy Agreement. See Section 7. Except for the CIA, however, which had already been using a Secrecy Agreement, other departments and agencies failed to carry out fully the mandate of the Section. Some agencies failed to require employees who already had access to execute agreements;

some agencies utilized Secrecy Oaths, rather than agreements, which are probably not judicially enforceable, see United States v. Marchetti, supra; some agencies did not require the Agreement of all employees because it would be demeaning or insulting to them; and some agencies are still trying to develop the language for a proper Agreement.

Even had the agencies fully complied with Section 7, there are certain inherent problems with Section 7 which render it fairly ineffectual even as to its limited objectives, i.e., to serve an additional educational and deterrent function and to serve as a basis for a civil injunction as in the Marchetti case. On the one hand, Section 7's Secrecy Agreement is limited to sources and methods; it does not cover classified information generally. In this respect the Agreement is underinclusive. On the other hand, the Agreement purports to protect all sources and methods, not just that which is classified, and it is doubtful whether a civil injunction can be obtained with respect to non-classified information, see United States v. Marchetti, supra. In this sense the Agreement is overinclusive.

For the above reasons, this subcommittee has recommended that Section 7 be deleted from E.O. 11905 and that the E.O. 11652 review should consider the

desirability of an improved Secrecy Agreement for possible inclusion in an amended E.O. 11652.

In any case, this subcommittee is of the view that a Secrecy Agreement will have only the most marginal, if any, effect on leaks of classified information. As noted above, the instances in which the Government will have prior knowledge of disclosure will be rare indeed and even in those cases courts will be loathe to enjoin broadly what the Government claims is classified. Moreover, the education and deterrent value of a Secrecy Agreement by itself is questionable; that is, it is doubtful that it would add anything to the secrecy oaths which have been required in the past, and, given the nature of the leaks in the past, it seems most unrealistic to think that a Secrecy Agreement would have deterred the leaks.

CONCLUSION:

Past experience indicates that there is an institutional unwillingness on the part of the Executive Branch to accept the costs and risks involved in criminal investigation and prosecution of leaks of classified information. On that basis, the enactment of new legislation to criminally punish the unauthorized disclosure of classified information would be a useless and politically costly exercise.

Because the decision whether or not to investigate or prosecute has in the past been made or not made haphazardly without interagency consideration of concerns beyond the immediate leak, the subcommittee recommends that the SCC require all agencies to report to it any leak which has or is about to be widely disclosed. The SCC as a group should then consider the merits of investigating that leak civilly or criminally not only in light of the particular leak but also in terms of the likelihood of success in investigation and prosecution and the deterrent effect on other leaks.

CENTRAL INTELLIGENCE AGENCY

WASHINGTON, D.C. 20505

1 JUN 1977

MEMORANDUM FOR: PRM/NSC-11 Subcommittee Members

FROM : 25X1
General Counsel

SUBJECT : Leaks of Classified Information

REFERENCE : Draft Report to the Special Coordination Committee
Same Subject, dated 27 May 1977, Prepared by DOJ

RECEIVED
JUN 1 5 36 PM '77
OFFICE OF LEGAL COUNSEL

1. I am not in general agreement with the conclusions and recommendations set forth in the referenced report. Nor do I believe those conclusions and recommendations reflect the positions expressed in the various papers submitted by the Subcommittee members, or in the Subcommittee discussions, relating to the subject of leaks.

2. The central conclusion in the draft report is that it would be fruitless to seek legislation prescribing criminal penalties for the unauthorized disclosure of classified information. That conclusion is said to be justified on the grounds that (a) the widespread cynicism in the Congress about the classification system would doom any proposed legislation that pegged criminal liability to Executive Order 11652 or otherwise defined a crime of "leaking" by reference to executive branch determinations that the information involved was classified, and (b) the facts that no prosecutions have been brought, and that few leaks have even been investigated, under the authority of existing laws, specifically the espionage statutes, would make it difficult if not impossible to explain the need for any new legislation, and indeed may demonstrate the absence of any such need. The same circumstances that have contributed to inaction in the past would, according to the draft report, likewise plague the administration of any new statute. One of these enumerated circumstances is the policy adopted several years ago by DOJ, which dictates a refusal to undertake any criminal investigation without an advance commitment from the concerned agency to declassify the information and documents determined to be essential for purposes of prosecution.

3. In my judgment the draft report does not fairly state the issues for consideration by the SCC. The fundamental problem is not, as the draft report would have it, an unwillingness to pay the price of enforcement of existing statutes. Rather the fundamental problem, which I believe the SCC must understand clearly, is that there is no criminal statute that is generally applicable, at least none that is clearly applicable, to the forms of



unauthorized disclosures characterized not by dealings with foreign agents and powers but rather by attributed publications or anonymous leaks to the press. An appreciation of the statutory vacuum that exists in this area is a necessary predicate for an informed decision by the SCC as to whether legislative initiatives are appropriate.

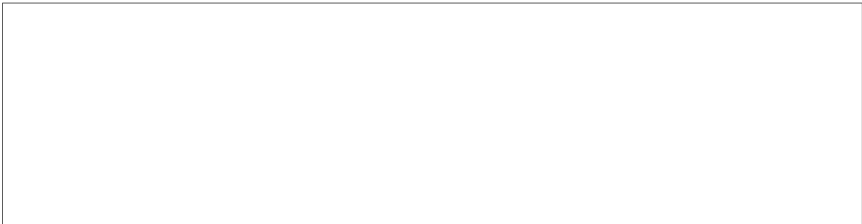
4. To be sure, as the draft report indicates, there are some narrowly drawn and specialized statutes, e.g., 18 U.S.C. §793 and 50 U.S.C. §783, that might support a prosecution under some circumstances, but their authority is concededly very limited. When it comes to the more broadly worded espionage statutes, 18 U.S.C. §§793(d) and (e), there is serious doubt, to put the best face on it, that they were ever intended to apply, or would be constitutional if they were applied (which as a matter of historical fact they have not been, with the lamentable exception of the Ellsberg case), to the conduct typically involved in the unauthorized leak. See generally the Espionage Statutes and Publication of Defense Information 73 Col. L. Rev. 929 (1973). The draft report is misleading in its implication that, assuming the leaked information qualifies as "information relating to the national defense," these provisions provide an adequate and legally supportable basis for prosecution.

5. Even assuming the state of existing law is as implied by the draft report, the pros and cons surrounding the DOJ investigative policy should be reviewed for the benefit of the SCC. The key policy, pursuant to which no criminal investigation can be authorized absent an advance commitment that the relevant information will be declassified, is neither necessary nor desirable in our opinion. Our views in that regard are outlined in a letter from former DCI Bush to former Attorney General Levi dated 1 December 1976, a copy of which is attached, and we believe these views should be laid before the SCC. That is especially important if the basic issue framed for the SCC is the alleged non-enforcement of existing statutes, rather than, as we perceive the true issue, the non-existence of any applicable statute.

6. Assuming further that the SCC accepts the draft report's formulation of the problem and accepts also the necessity of requiring declassification decisions prior to investigation, there are a number of alternatives to the do-nothing approach recommended in the draft report. Legislation along the lines of the bill drafted by DOJ in March, which formed the basis for the earlier deliberations of the Subcommittee, is one such alternative. That legislation, as we understood it, would have defined an offense in terms such that the Government would not be required to prove the underlying significance of the leaked information. That is, under this proposal, the validity of classification would not be an element of the offense, so long as there existed

a procedure for the independent review of the information, through which the need for continued classification could be tested prior to its disclosure and so long as the defendant did not avail himself of the procedure. Another alternative would be legislation along the lines of H.R. 12906, as introduced in the 94th Congress, which would not make punishable the unauthorized disclosure of all classified information but rather would create a narrower category of protected information, and which would leave the critical evaluations as to the quality of that information to in camera determinations by judges rather than determinations by juries following an open presentation of evidence. None of these alternatives, or any variation thereof, is even mentioned in the draft report, let alone discussed.

7. As matters now stand, national secrets can be leaked with impunity, and we are all frequent witnesses to such conduct. It may be that after full and measured consideration, the SCC would elect to accept the status quo, essentially as recommended in the draft report, even though there is something more than slightly ludicrous about a situation in which a government employee is legally free to divulge information gravely damaging to the national security but is subject to criminal penalties if he discloses, for example, crop information, 18 U.S.C. §1902, or, be he a bank examiner, the names of depositors or collateral for loans of any member bank of the Federal Reserve System, or bank insured by the FDIC, 18 U.S.C. §1906. At a minimum, however, any such decision by the SCC to accept the status quo should only be made in the context of a complete understanding of the present realities, and the range of possible options, which in our view the draft report does not adequately describe.



25X1

Executive Registry
76-8010

1 DEC 1976

The Honorable Edward M. Levi
Attorney General of the United States
Department of Justice
Constitution Avenue and Tenth Street, N.W.
Washington, D.C. 20530

Dear Sir:

As you are aware, unauthorized disclosures of sensitive intelligence have reached epidemic proportions. In previous correspondence and in conversations with you and Mr. Kelley, I have expressed my concern over this matter and I am certain you share my apprehension. The Intelligence Community agencies have examined a number of potential remedial actions to solve, or at least abate, this problem. One of the most fundamental remedial actions, I believe, is an immediate and comprehensive investigation to determine the identity of those responsible for the unauthorized disclosures. Unfortunately, this is not possible today. While Intelligence Community security components react promptly to leaks within their limited spheres of authority, it is the Federal Bureau of Investigation (FBI) upon which we must rely for the extensive type of investigation required in these cases. It appears to me that the FBI is severely hampered by Department of Justice procedures in proceeding with cases of this variety.

I have been informed that before personnel of the FBI can conduct an investigation involving an unauthorized disclosure of classified information, they must obtain Department of Justice approval. I am advised that Department of Justice approval is predicated in each instance upon a determination that the compromised material will be declassified for prosecution purposes.

(ENCLOSURE)

OS 6 4814

These procedures create a dilemma in which the more sensitive the unauthorized disclosure, the less likely it is that a swift, energetic investigation will be conducted. Obviously there will be instances in which it will be appropriate to declassify a document in order to prosecute. However, the decision to prosecute should be made only when it is to the net advantage of the U.S. Government to do so. In many cases, the declassification decision must be based in part on the facts of the leak, which cannot be known without an investigation. In cases where prosecution may not be desirable, the investigation may identify persons responsible for the leak so that administrative action can be taken. In some instances, although the identity of the person responsible for the leak may not be obtained, the investigation will nevertheless provide valuable insight into the vulnerabilities of our security procedures or ways to better protect our vital intelligence secrets.

Upon investigation it may be determined that a given leak may not be a prosecutable offense. In those cases, declassification decisions will not be involved. Knowledge of the facts and circumstances of the case together with the identity of the source of the leaks is still important.

I would appreciate your considering the initiation of more streamlined procedures which would enable the FBI to act promptly in investigating an unauthorized leak which is reported to the Bureau by any agency of the Intelligence Community. In particular, I suggest that the agency involved be given the option to defer the decision whether to declassify information involved until sufficient investigation has been conducted which would permit a fully-informed, rational determination. It is recognized that the decision to prosecute is a matter of discretion by the Department of Justice, taking into account a wide range of government interests, the rights of individuals, fairness, etc. The protection of intelligence sources and methods is one such interest of the government.

I would be very happy to meet with you personally on this matter, which I consider to be of most urgent interest to the Intelligence Community. Or, if you desire, I would welcome an opportunity for members of my Offices of General Counsel and Security to meet with your representatives to discuss new procedures in these cases.

Sincerely,



25X1

George Bush



DEPARTMENT OF DEFENSE
OFFICE OF GENERAL COUNSEL
WASHINGTON, D. C. 20301

June 2, 1977

MEMORANDUM FOR Mr. John Harmon
Acting Assistant Attorney General
Department of Justice

FROM Robert T. Andrews *RTA*
Senior Advisor to the General Counsel

Because of the time constraints*, the Department of Defense has deferred submitting a redraft of the proposed Report to the Special Coordination Committee on "Unauthorized Disclosure of Classified Information". Instead, the DoD comments will address only those portions of the Report in which it takes a somewhat different position.

Investigation and Prosecution Under Current Laws.

The DoD perceives a need to place greater emphasis, in selected leak cases, on prompt and vigorous investigations. Continued failure to investigate the more flagrant disclosures is self-defeating. One impediment in initiating an FBI investigation is the DOJ's insistence that the DoD, as well as other Agencies, agree in advance to declassify the information for purposes of prosecution. While the DOJ must necessarily husband its investigative resources, it addresses the problem solely in terms of its prosecutive interests. On the other hand, the Departments and Agencies whose sensitive information has been leaked, address the problem in terms of their management

* The May 27, 1977 proposed Report was received by DoD on May 31, 1977. It was immediately disseminated for comment to the Military Departments and Defense Agencies concerned with intelligence, investigations and classification, and a meeting scheduled for the following day. At that meeting, substantial revisions and editing of the Report were recommended. However, at the request of the Subcommittee Chairman last evening, DoD is submitting a summary of its position, rather than a rewrite of certain portions of the Report.

interests, i.e., what are the facts behind the leak, what caused the leak, and what corrective management actions are called for. As a consequence, these competing interests often result in a stalemate. Thus, neither law enforcement nor management interests are served.

DoD and ERDA are presently engaged in discussions with the DOJ regarding the requirement for an advance commitment to declassify information about warhead designs, yield and reliability prior to an investigation. The disclosures primarily involve Restricted Data and Formerly Restricted Data, and the only means of resolving the impasse appears to be through direct communication between the Heads of the interested Departments. While this particular matter is not one appropriate for resolution by the Special Coordination Committee, the Committee could direct that appropriate Government-wide guidelines be drawn up which would permit an accommodation of the views expressed above. One suggested remedy would be to authorize the FBI to conduct what is essentially a "civil investigation", as distinguished from a "criminal investigation".

Introduction of New Criminal Legislation.

The DoD components concluded that legislation making it a crime for a Government official to disclose classified information in an unauthorized manner would have a deterring effect, if enacted. It was also noted that the legislation, if properly drawn, would pass constitutional muster.

It has been DoD's experience that the present criminal statutes involve substantial problems of proof (e.g., the Government must show harm to the United States or benefit to a foreign power), and risks of disclosure of classified information during the course of a public trial. Further, it has found that the present laws are not designed for use in security leak cases in which there is no suggestion of deliberate espionage. Consequently, the Government's failure to "utilize the laws now available" does not necessarily lead to the conclusion that no new legislation should be sought.

New legislation, carefully drafted, could eliminate certain though not all of the present areas of concern. However, such a legislative proposal is inalterably linked to the security classification process. Unless the security classification system is policed, and applied

judiciously and with restraint, there is little likelihood of convictions under such a statute. The classification study directed by PRM/NSC-29 of June 1, 1977 represents a proper step in this direction.

Of more immediate importance, however, is whether such a legislative proposal could be enacted by the Congress. Obviously, any new criminal legislative proposal of this nature would stir up immediate Congressional opposition from some quarters, and would involve considerable "political costs" in securing enactment. The Vice President's recommendation that civil, rather than criminal sanctions be pursued, should be considered before electing to introduce a criminal statute. While civil fines would normally require legislation, consideration should be given to including in the Secrecy Agreement prescribed by Section 7 of E.O. 11905, a provision calling for liquidated damages, at least in those instances in which code word material is involved.

Additionally, the Head of Departments and Agencies of the Executive Branch should be reminded of the requirement to "take prompt and stringent administrative action" against security leak offenders. See Section 13(B) of E.O. 11652 and the National Security Council Directive of May 17, 1972 implementing that Order. Unless and until these and other administrative steps are taken, Congress will surely turn a deaf ear to new legislation.

The CIA Memorandum of June 1, 1977 correctly describes the existing state of affairs as a "statutory vacuum", and properly notes the absence in the Report of any discussion of already drafted legislative proposals to impose criminal sanctions for leaks of national secrets. However, unless Congress is motivated to act because of new and startling national security disclosures, it is very unlikely that such legislation will be favorably received.

Use of Secrecy Agreements

Contrary to the representations in the Report, a number of DoD components has required the execution of Secrecy Agreements for a number of years. In some instances, the Agreement is confined to employees having access to intelligence sources and methods; in other versions, it also extends to those having any access to classified information. The components using such agreements include the Office of the Secretary of Defense, the Defense Intelligence Agency,

the National Security Agency, certain intelligence elements of the Military Departments, and employees of certain DoD contractors involved in "special access" programs.

DoD believes that these agreements have educational value and serve as a deterrent. The terms of the Secrecy Agreement previously presented by DoD, and concurred in by DOJ, should be considered for Government-wide adoption. In our view, Section 7 of E.O. 11905, calling for Secrecy Agreements, should not be repealed until such time as E.O. 11652 is repromulgated, at which point this requirement can be incorporated in the Security Classification Order.

Copies to: Herbert J. Hansell
Legal Adviser
Department of State

25X1

General Counsel
Central Intelligence Agency

W. Bowman Cutter
Executive Associate Director for Budget
Office of Management and Budget

Samuel C. Hoskinson
Staff Member
National Security Council

John B. Hotis
Legal Counsel
Federal Bureau of Investigation

Frederick A. O. Schwarz, Jr.
Office of the Vice President

Executive Summary

The Freedom of Information and Privacy Acts

The attached report contains the recommendations to the SCC of the PRM-11 Subcommittee concerning the Freedom of Information ("FOIA") and Privacy Acts.

Four issues were considered with respect to the FOIA. These issues and the recommendations concerning them were as follows:

(a) The administrative burden imposed on the Government in general and the fact that with respect to intelligence agencies very little material of general public interest is made available because of the necessity of protecting classified information and sources and methods, all of which are exempt from mandatory disclosure. A related problem is the accumulation of materials concerning requests which results from the lack of a statute of limitations for suits challenging denials. The subcommittee believes that nothing can be done at this time to alleviate this problem. The Department of Defense dissents with respect to the statute of limitations.

(b) Exposure of classified material in in camera judicial inspection and though acknowledging that an exempt record exists, since in some cases making the mere existence of a record known, may well in itself disclose classified information.

(c) The incongruous fact that foreign requesters are not excluded from making FOIA requests and thus can burden the intelligence agencies. The subcommittee believes that legislation excluding foreign source requesters from using the FOIA would be appropriate.

(d) The language in the Court of Appeals decision in Weissman v. CIA, which suggests that the CIA cannot lawfully investigate unwitting American citizens who are unconnected with the CIA. The subcommittee believes that this is a problem of the CIA's authority and not an FOIA problem.

With respect to the Privacy Act, the subcommittee considered five issues:

(a) The lack of an exemption for inter- and intra-agency memoranda which results in a stifling of candid discussion. In light of the fact that this issue was raised at the time the Privacy Act was enacted, the subcommittee believes that nothing can be done at this time to alleviate this problem. The Department of Defense dissents.

(b) The concern that foreign government sources raise with respect to the possible disclosure of information furnished in confidence. The subcommittee is of the opinion that this fear is unfounded in that existing exemptions should suffice to protect this information.

(c) The inhibiting effect the required Privacy Act disclosure has in pursuing foreign intelligence leads. The CIA has the power to exempt itself from this requirement and the subcommittee believes that a similar exemption should be sought with respect to intelligence agencies of the Department of Defense and the Security Office of the Department of State.

(d) The confusion caused by the current LEAA regulations and underlying statute with respect to the furnishing of state and local police records to Federal agencies in connection with personnel security investigations. The subcommittee believes that the problem can only be rectified by amending the statute. The Department of Defense dissents and recommends amendment of the LEAA regulations.

(e) The administrative burden imposed by the Act. The subcommittee does not believe that it would be worthwhile for the intelligence agencies to attempt to get a broad revision of the Act.

Report to the Special Coordination Committee Concerning
the Impact of the Freedom of Information and Privacy Acts
on the Intelligence Community

1. Freedom of Information Act

(a) Administrative Burden

(i) Issues

A universal complaint about the Freedom of Information Act (5 U.S.C. §552) ("FOIA") is that the Act imposes an excessive administrative burden upon government agencies. Thus, for example, the CIA's direct labor costs of responding to FOIA requests during calendar year 1976 exceeded \$740,000 and those of Defense exceeded \$4,720,000. Furthermore, in all agencies a substantial amount of senior management time is devoted to FOIA matters, at the expense of what management believes to be the primary duties of the agencies. It is also noted that little of public interest is released by the intelligence agencies because the sources and methods statutes (50 U.S.C. §403(d)(3), 403(g)) fall within exemption 3 of the FOIA (5 U.S.C. §552(b)(3)) and the fact that much of the material in the files of these agencies is classified and thus exempt from mandatory disclosure by exemption 1 (5 U.S.C. §552(b)(1)).

*/ The Department of State believes that the problems with the FOIA are not unique to intelligence agencies and that the President should establish an Executive branch committee to determine what revisions to the FOIA might be appropriate.

Particularly in the case of FOIA requests for information about intelligence operations or specific topics of intelligence interest, as opposed to requests by individuals for access to their own files, an enormous amount of effort is expended to produce a very limited amount of releasable information.

The lack of a statute of limitations for FOIA suits adds to the burden. Agencies are now required to maintain files relating to FOIA denials indefinitely because there is no time limit within which suits must be commenced.

(ii) Options

(A) Accept present situation.

(B) Seek legislation establishing an exemption modeled on exemption 7 as it was before the 1974 Amendments exempting certain intelligence files from mandatory disclosure.

(C) Seek legislation exempting intelligence agencies from the requirement that reasonably segregable portions of otherwise exempt materials be made available.

(D) Seek legislation establishing a short statute of limitations for suits challenging FOIA denials.

(iii) Recommendation

Do nothing. The prospects for legislation in this area do not appear promising at this time. Congress has heard the burden

argument at length and has not appeared particularly moved. The argument that other responsibilities are slighted lacks impact because proof of its truth or examples of its consequences depend, in effect, upon proving a negative; i.e. that certain activities were not being carried out because of the time devoted to FOIA matters. The burden appears here to stay, at least for the foreseeable future. However, in connection with oversight hearings and on similar occasions, the opportunity should be taken to begin to educate Congress about the problems in this area and, in time, consideration should be given to a narrow exemption aimed at the peculiar circumstances of the intelligence agencies.

The statute of limitations problem seems relatively minor.^{*/} Furthermore, the preservation of files relating to denials seems generally desirable in that it increases the likelihood of consistent responses when similar requests are received.

(b) Possible Compromise of Classified Information

(i) Issues

There is some concern over the possible compromise of classified information during the course of in camera judicial review pursuant to FOIA. To date this problem remains theoretical; nevertheless, it may be appropriate to direct the Freedom of Information and Privacy Section of the Justice Department's Civil Division to be certain to apprise a judge to whom classified

^{*/} The Department of Defense dissents. See Appendix A.

information is transmitted of the requisite security requirements. The usual present practice of strenuously resisting such review in intelligence cases, largely successful to date, provides a first line of defense and should be continued.

A more difficult problem is presented by the situation in which acknowledging that an exempt record exists in order to deny an FOIA request discloses classified information. Thus, for example, NSA notes that merely claiming an exemption in response to an FOIA request gives rise to an inference NSA was able to decipher some communication relating to the request. This problem is, of course, somewhat similar to the one which faced the CIA when requests were made to it for documents relating to the Glomar Explorer. To claim an exemption for any such documents would be to acknowledge their existence as CIA records and implicitly to acknowledge some connection between the ship and the CIA. In those cases the CIA successfully took the position that the very existence of the documents was, in effect, classified and exempt from disclosure under exemptions 1 and 3 (5 U.S.C. §552(b)(1), (3)). Phillippi v. Central Intelligence Agency, 484 F.2d 820 (D.C. Cir., 1975); Military Audit Project v. Bush, 418 F.Supp. 876 (D.D.C. 1976). This approach

is also being used in connection with some pending cases involving signals intelligence and communications security.

(ii) Options

(A) Continue present practice.

(B) Seek legislation specifically sanctioning agency refusal to state whether or not a record exists on the ground that such a statement would disclose classified information.

(iii) Recommendation

The Phillippi approach has been effective so far in dealing with situations where disclosure of the existence or non-existence of a record would reveal classified information and where the agency in question has been prepared to provide affidavits to that effect. Therefore, there does not appear to be any need for legislation in this area at this time.

(c) Foreign-Source Requests

(i) Issues

The fact that foreign requesters can impose a substantial burden on an agency and obtain agency documents is galling to many, and ingenious arguments have been made for excluding foreign requesters from the benefit of the FOIA as it now is. Unfortunately, all of these arguments run into the definition

of "person" in 5 U.S.C. §551(2) which clearly does not exclude foreigners not resident in the United States. While the Privacy Act (5 U.S.C. §552a) is limited to citizens and aliens lawfully admitted for permanent residence, the same is not true of the FOIA. Because of the overlap between these two Acts, it is possible to avoid the Privacy Act limitation by making an FOIA request.

(ii) Options

(A) Do nothing.

(B) Seek legislation limiting FOIA access to citizens, aliens lawfully admitted for permanent residence and associations organized in the United States and having their principal place of business within the United States; see, e.g., 22 U.S.C. §611 (b)(3).

(C) Seek legislation making the Privacy Act the exclusive vehicle for requesters seeking information about themselves.

(iii) Recommendation

Seek legislation of the type described in (ii)(B), supra. This appears to be the narrowest way to attack a problem which the intelligence community finds to be a significant irritant. Adoption of the approach in (ii)(C) would have broader consequences than necessary in that some information about themselves

available to U.S. citizens under the FOIA may not necessarily be available under the Privacy Act, and vice versa. Thus, such an amendment would probably face a more difficult legislative passage and would, indeed, be broader than is necessary to meet the concerns to which it is addressed.

One difficulty with this recommendation is that it raises the unpalatable possibility of the investigation of FOIA requesters. Another is that the case to be made for the amendment depends more upon the illogic of permitting non-U.S. requesters to impose upon the Government than upon any demonstrable harm to it. Nevertheless, sound arguments can be made for such an amendment.

(d) The Weissman Case

(i) Issues

In Weissman v. CIA, Civ. Act. No. 76-1566, D.C. Cir., January 6, 1977 amended and rehearing denied April 4, 1977, the court indicated, in connection with holding that exemption 7 was unavailable to the CIA in connection with records generated concerning the investigation of unwitting American citizens within the United States who are unconnected with the CIA, that the CIA does not have authority to conduct such investigations.

This, of course, creates two related problems for the CIA: first, it brings into question the CIA's authority to make such investigations, notwithstanding the uninterrupted practice of twenty years and the fact that such authority has never previously been called into question; second, it denies the protection of exemption 7 to records generated in connection with such investigations.

(ii) Options

(A) Do nothing in the FOIA context.

(B) Seek legislation amending exemption 7 to include lawful investigations of persons reasonably believed to be potential sources or contacts.

(iii) Recommendation

Do nothing in the FOIA context because the problem is not an FOIA problem. Amendment of exemption 7 would not address the more fundamental problem of the effect of this decision on the CIA's authority, which is the proper context within which to deal with this matter.

2. Privacy ^{*/}

(a) Lack of Inter- and Intra-agency Exemption

(i) Issues

The Privacy Act (5 U.S.C. §552a) contains no exemption for inter- and intra-agency memoranda. Therefore, for example, evaluative memoranda in a person's personnel file are ordinarily available to the person who is the subject of such evaluation. It appears that the possibility of such access substantially inhibits candid evaluation, a problem which becomes particularly acute with respect to the granting of security clearances.

(ii) Options

(A) Do nothing to attack this as an isolated problem.

(B) Seek legislation exempting such evaluations from disclosure under the Privacy Act.

(iii) Recommendation

Do nothing.^{**/} This problem was brought to the attention of the appropriate Congressional committees when the Privacy Act was under consideration and the suggestion that an exemption would be appropriate did not receive a favorable reception.

^{*/} Because of the CIA's broad power to exempt itself from various provisions of the Privacy Act (5 U.S.C. §552a(j)(1)) the greater part of this discussion is inapplicable to it.

^{**/} The Department of Defense dissents. See Appendix A.

While the problem has now passed from the realm of prediction to that of fact, there is no reason to believe that a different legislative result would obtain today. It appears that the most feasible way to alleviate this problem is to encourage evaluators to be as frank as possible, notwithstanding the fact that the subject may have access to evaluative material. Others within the government, for example judges before whom cases are being tried or in the course of sentencing, must frequently make candid personal evaluations which will be available to the subject; nonetheless, they manage to do their duty as they see it.

(b) Inhibition of Foreign Agencies

(i) Issues

Foreign governments frequently provide information on the express condition that the identity of the source and the substance of the information be kept confidential. So far the use of the classification exemption (§552a(k)(1)) and the confidential source exemption (§552a(k)(5)) has sufficed to preserve confidentiality but some concern arises that the (k)(5) exemption might apply only to individuals and not to agency sources.

(ii) Options

(A) Do nothing and rely upon the position that foreign governments may be confidential sources.

(B) Seek legislation specifically protecting foreign governments.

(iii) Recommendation

Do nothing. The Department of Justice is of the view that the (k)(5) exemption can include foreign agencies and that the fear expressed by the foreign governments is unfounded. In the absence of a contrary judicial interpretation, no legislation is needed to deal specifically with this problem. To a considerable degree it should be ameliorated by providing such assurances as may be necessary to the agencies furnishing information.

(c) Required Disclosure in Seeking Information

(i) Issues

Agencies seeking information about a person generally are required to do so openly and to provide a Privacy Act statement (5 U.S.C. §552a(e)(3)). The CIA and law enforcement agencies have the power to exempt themselves from this requirement. However, the Department of Defense and the Department of State cannot exempt themselves and thus are prohibited from making "under cover" approaches to persons within the protection of the Act. As a result, the intelligence components of the Department of

Defense and the Security Office of the Department of State are restricted in their ability to pursue foreign intelligence leads.

(ii) Options

(A) Do nothing.

(B) Attempt to take advantage of the CIA's (j)(1) exemption by having the CIA claim ownership of all such records and having other agencies maintain them as, in effect, custodian.

(C) Seek legislation making the (j)(1) exemption power available to all intelligence agencies.

(iii) Recommendation

Legislation making the (j)(1) exemption power available to all intelligence agencies should be sought. In order to make such legislation more palatable to Congress, it might be desirable to limit the scope of the exemption sought in a manner similar to that in which the CIA has limited its exemption under (j)(1). Alternatively, in the event that the proposals now under consideration to reorganize the intelligence functions of the government lead to a decision to do so, the possibility of effecting such a reorganization in such a manner as to make the benefit of the (j)(1) exemption available where appropriate should be given consideration.

With respect to the proposed use of the CIA's exemption by other agencies, in the absence of a reorganization, it is argued that a similar arrangement is in effect with respect to certain Civil Service Commission records, but of course, the fact that those records belong to the Civil Service Commission does not result, as it would in the proposal under discussion, in exempting the CSC records from substantial parts of the Act. The Department of Justice is of the opinion that such an attempted use of the CIA's exemption would be a mere sham and an improper evasion of the Act.

(d) Access to State and Local Criminal Information

(i) Issues

Presently, the LEAA regulations governing access to criminal justice information systems refer back to state law to determine what information can be made available to Federal agencies in connection with personnel security investigations. Additionally, DIA suggests that state and local agencies are uncertain of the proper interpretation of the LEAA regulations and thus deny access even in jurisdictions where state law does not prohibit such dissemination.

(ii) Options

- (A) Do nothing.
- (B) Amend LEAA regulations.
- (C) Seek legislation amending the underlying statute to authorize the disclosure of such information.

(iii) Recommendation

Amend the statute. */ The Department of Justice does not believe that amendment of the LEAA regulations is an appropriate means of dealing with this problem and that the matter must be dealt with by amendment of the statute. Such an amendment would be appropriate and should be sought.

(e) Administrative Burden

As is the case with FOIA, all agencies complain about the frequently pointless administrative burden imposed by the Privacy Act, particularly the publication requirement and even more particularly the annual republication requirement; for example, there seems to be little public benefit in requiring each agency annually to publish a notice about the fact that it has a payroll. This, however, is not a problem peculiar to agencies in the intelligence community and it is doubtful that it would be worthwhile for such agencies to devote their efforts to a broad revision of the Act.

*/ The Department of Defense dissents. See Appendix A.



DEPARTMENT OF DEFENSE
OFFICE OF GENERAL COUNSEL
WASHINGTON, D. C. 20301

June 2, 1977

MEMORANDUM FOR Mr. John Harmon
Acting Assistant Attorney General
Department of Justice

SUBJECT: Report to the SCC re the Freedom of Information
and Privacy Acts

The following comments are submitted regarding subject report.
Except for the comments set forth below, we concur in the report
as written.

1. FOIA Statute of Limitations: The Justice Department memorandum disposes of the need for a statute of limitations on FOIA denial litigation by asserting that the problem "seems relatively minor." It also noted that the presumably indefinite retention of denial files is desirable because it increases the likelihood of consistent responses in similar cases. The Department of Defense disagrees with this analysis in two respects. First, the number of FOIA requests denied by agencies will obviously continue to accumulate over the years. Secondly, under regulations issued by the Administrator of General Services pursuant to Chapter 33 of title 44, United States Code, federal agencies usually retain records locally only for a fixed time. A reasonable statute of limitations would be consistent with the Freedom of Information Act and compliments the Privacy Act's purpose of limiting the amount of information maintained on individuals.

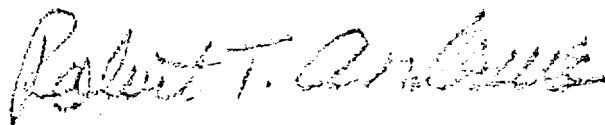
2. Foreign-Source Requests: The Department of Defense concurs with the Justice Department's recommendation that legislation be sought to limit FOIA access to citizens, aliens lawfully admitted for permanent residence and United States associations as described. We believe this recommendation reflects the original Congressional intent and would also be consistent with the Privacy Act. Since eligibility for access to records could be determined simply by reference to the information on the face of the request, we foresee no problem with determining the identity of FOIA requesters.

3. Lack of Inter- and Intra-agency Exemption: There is no exemption for inter- and intra-agency memorandums in the Privacy Act. The Department of Justice recommendation is to do nothing. The Department of Defense believes that this problem is significant and that additional consideration should be given as to whether a legislative change could be obtained. The problem is not limited solely to the evaluative comments in personnel files but extends to other matters which fall within the traditional attorney-client and executive privileges. An amendment, if drawn narrowly, could balance the needs of agency deliberative processes and the policy of providing an individual access to information pertaining to himself.

4. Access to State and Local Criminal Information: The Department of Justice recommends a statutory amendment be sought to authorize the disclosure of state criminal justice information to Federal agencies. The Department of Defense believes that the result sought can be achieved merely by amending Law Enforcement Assistance Administration regulations. The Justice Department disagrees but provides no basis for its conclusion. We continue to recommend LEAA regulations be amended to:

a. Spell out the legitimacy of Federal investigative agency need for criminal history information in connection with access to classified information, assignment to sensitive positions and entry into the Armed Forces.

b. Provide for allocation of LEAA funding support when inability of state and local agencies to meet the Federal need for criminal history information is due to insufficient funds.



Robert T. Andrews
Senior Advisor to the General Counsel

Executive Summary

The attached report is submitted to the SCC by the subcommittee acting under the direction of the Attorney General pursuant to PRM/NSC-11.

The subcommittee has scrutinized E.O. 11905 to determine what changes, if any, were deemed necessary in light of the past year's experience. The subcommittee did not address Section 3 of the Order, relating to the Control and Direction of Intelligence Organizations, nor did it address substantive questions concerning the organization or functions of the Intelligence Community. The President has indicated to the Senate Select Committee that the Administration will not act unilaterally to pre-exempt the Congressional effort to address these questions in charter legislation.

Rather the subcommittee has identified drafting errors in E.O. 11905, provisions which in practice have been found too ambiguous, and certain specific provisions which in practice are felt now to be inappropriate. The subcommittee recommends that the appropriate changes to E.O. 11905 be effected as soon as possible, because certain provisions of the Order are not being followed because of these problems and other provisions as now drafted raise grave legal questions with regard to current operations and procedures. The subcommittee does not believe that its recommended changes can be viewed as undercutting or predetermining later decisions by the Executive or Congress relating to intelligence agencies' functions or the intelligence community's organization. Therefore, the subcommittee is of the view that these changes and the reasons for them can be explained to the Senate Select Committee and then be effected immediately by amendment to E.O. 11905 consistent with the Administration's commitment to cooperate with the Congress on charter legislation.

With one exception the subcommittee recommends specific changes to the Order. The one exception (see pages 18-43) involves Section 4(a)(5) of the Order, which requires all intelligence agencies to report to the Attorney General "that information which relates to detection or prevention of possible violations of law by any person, including an employee of

the. [intelligence] department or agency." While the subcommittee is agreed that this provision is too broad, there is substantial disagreement as to its proper scope.

The CIA recommends that Section 4(a)(5) be deleted entirely, thereby putting intelligence agencies under the same statutory obligation as any other governmental agency to report only violations of the law by employees of the agency, see 28 U.S.C. § 535(b), (see Option 1, pages 21-28), or if this is not acceptable, that the provision be limited to require reporting only where crimes under title 18 by government employees or a specified list of crimes by U.S. or foreign intelligence agency operatives are involved (see Option 3, pages 39-42).

The Department of Justice recommends that the Section 4(a)(5) reporting requirement be limited to a list of "serious" crimes where case-by-case determinations whether to prosecute must be made by weighing the competing interests of law enforcement and the threat to intelligence sources and methods, but that information concerning these violations by any person would have to be reported to the Attorney General so that the prosecutorial decision would continue to be made by the Attorney General.*/ (see Option 2, pages 29-39).

The Department of Defense recommends that Section 4(a)(5) be amended to allow the Attorney General by regulation to exempt the reporting of certain crimes or of crimes generally in certain circumstances (see Option 4, pages 42-43).

The specific recommendations agreed upon by the subcommittee are as follows:

Drafting Errors:

(1) Redefinition of foreign intelligence and counter-intelligence to have one definition for the entire Order, rather than the two different definitions that now exist (pages 3-4) (page references are to the attached report of the subcommittee).

(2) Elimination of an inadvertent restriction on CIA having counterintelligence authority (page 4).

*/ The Department of State concurs in this recommendation.

(3) Addition of a requirement for CIA to coordinate with the FBI in CIA's foreign intelligence clandestine collection in the United States (pages 4-5).

(4) Addition to Defense's charter to acknowledge the existence and duties of the intelligence components of the military services and the existence of a DoD foreign counter-intelligence mission (pages 5-7).

(5) Addition to the FBI's charter to acknowledge its occasional activities overseas, its responsibility to detect and prevent international terrorism, to eliminate the terms "espionage, subversion and other unlawful activities" and substitute "clandestine intelligence activities" (pages 7-8).

(6) Clarify Section 5's preamble to acknowledge intelligence agencies' legitimate interest in foreign organizations and persons (page 8).

(7) Clarify definition of "foreign intelligence agency" (page 9).

(8) Clarify definition of "physical intelligence" (page 10).

(9) Allow collection and dissemination of information about domestic activities of U.S. persons reasonably believed to present a danger to a Secret Service protectee (page 11).

(10) Permit dissemination of incidentally acquired information relating to state, local, and foreign crimes to state, local, and foreign law enforcement agencies (pages 11-12).

Ambiguities:

(1) Define "International Terrorist Activities" (page 13).

(2) Clarification of the restriction on intelligence agencies' participation in law enforcement (pages 13-17).

(3) Clarification of the location and funding of and timing of reports to the IOB (pages 17a - 17b).

Policy Differences:

(1) Inclusion of a charter for the Drug Enforcement Administration's intelligence activities (pages 43-45).

(2) Allowing intelligence agencies to assess the suitability of a person for recruitment or contact by participating in a domestic organization (pages 45-46).

(3) Deletion of Section 7 of the Order relating to Secrecy Agreements (pages 47-48).

REPORT TO THE SPECIAL COORDINATION COMMITTEE

Re: Executive Order 11905.

The following report is submitted to the Special Coordination Committee pursuant to PRM/NSC-11 by the subcommittee acting under the direction of the Attorney General. The report is made at this time in an attempt to facilitate the work of the PRM/NSC-11 Section 3 review. This report does not address Section 3 of Executive Order 11905, which is under the jurisdiction of the subcommittee chaired by the DCI.

In the year since E.O 11905 was promulgated, certain drafting errors have been identified, ambiguities in certain language have made their impact felt, and certain deliberate inclusions in and exclusions from that Order are now questioned. A recommendation has been

made by the Vice President that no changes be made to E.O. 11905 for six months to demonstrate the Executive's good faith with respect to the drafting of legislative charters. The subcommittee believes, however, that none of the changes recommended in this report would undercut the Executive's good faith with respect to statutory charters for intelligence agencies. None of the changes recommended, taken individually or collectively, represent substantive decisions on the functions, responsibilities, or restrictions relating to intelligence agencies. They are invariably recommendations to correct drafting errors, ambiguities, or specific problems with specific provisions of the Order.

Moreover, several of the matters about which recommendations are made deserve, if not demand, immediate treatment, e.g., the reporting requirement of Section 4(a)(5) and the Secrecy Agreement of Section 7 (because of widespread failure to abide by the provisions of the Order), the lack of any authority for military counterintelligence activities, and the lack of any specific exception for information to be disseminated to the Secret Service or to

" local law enforcement agencies. It is the recommendation of the subcommittee that in the spirit of cooperation with the Congress in the legislative charter effort, the Senate Select Committee be informed of these proposed modifications in E.O. 11905 and that the President issue an amendment to effect the following changes.

I. Drafting Errors

(1) Section 2(a) -- This subsection defines intelligence in two paragraphs, the first of which defines foreign intelligence and the second of which defines foreign counterintelligence. Section 5 of the Order, because it was drafted by a different task force, defined these same terms in a different manner. A single definition for each term should be used for the entire order.

The subcommittee recommends that the definition of "foreign intelligence" and "counterintelligence" be deleted from Section 5 and Section 2(a) be amended to read:

"(a) Intelligence means:

(1) Foreign intelligence, which means information, other than foreign counterintelligence, relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons; and

(2) Foreign counterintelligence, which means information gathered as well as activities conducted

to protect against espionage and other clandestine intelligence activities, sabotage, international terrorist activities, and assassination conducted for or on behalf of foreign powers, organizations, or persons, and to protect intelligence or national security information and its means of collection from detection or disclosure, but not including personnel, physical or document security programs."

(2) Section 4(b) -- The preamble to CIA's charter in the Executive Order states that all its duties and responsibilities must be related to the "foreign intelligence functions" outlined in Section 4(b). The term "foreign intelligence," however, is a defined term in the Order which does not include counterintelligence, which is one of CIA's functions in Section 4(b). Therefore, the subcommittee recommends that Section 4(b) be amended by deleting the word "foreign" where it appears before "intelligence functions."

(3) Section 4(b)(2) -- Under this paragraph CIA is authorized to engage in the clandestine collection of positive foreign intelligence both within and without the United States, in accordance with NSC directives. When it engages in such collection in the United States, in

practice it coordinates its activities with the FBI pursuant to a written agreement to insure that neither organization's activities are compromised. This type of coordination should be recognized in this paragraph as it is in other sections, see, e.g., Section 4(b)(4).

The subcommittee recommends that the paragraph be amended by inserting after the last word: "and in the United States in coordination with the FBI."

(4) Section 4(e) -- The intelligence components of the military services have traditionally engaged in foreign intelligence and counterintelligence activities at home and abroad in support of DOD components, usually military commands, as well as national intelligence requirements. The Executive Order did not intend to eliminate this traditional role, but due solely to drafting oversight the intelligence elements of the military services were omitted from Section 4(e), although denominated as members of the Intelligence Community in Section 2(b)(5). And again due solely to a drafting oversight no counterintelligence function was specified in the Department of Defense charter at all. This has raised a substantial legal question whether DOD can continue to engage in any counterintelligence

Sanitized Copy Approved for Release 2011/01/26 : CIA-RDP79M00095A000300010001-0

activities if the Order is not amended to provide specifically for a DOD counterintelligence function because the Department of Justice interprets the Order as the exclusive charter of the intelligence functions of the several specified departments and agencies.

The subcommittee recommends that Section 4(e)(1) be amended to add a new paragraph to read:

"(vii) Conduct foreign counterintelligence activities worldwide in support of Department of Defense components, in coordination with the FBI in the United States and in coordination with the CIA overseas."

And section 4(e)(2) be amended to add a new paragraph to read:

"(iv) The intelligence and counterintelligence elements of the military services whose respective functions, authorities and responsibilities shall include:

(A) The collection, production, and dissemination of foreign intelligence in support of military commands and departments, the Department of Defense, and national intelligence requirements, provided that, the collection abroad of foreign intelligence information, not otherwise obtainable, shall be coordinated with the CIA.

(B) The conduct of foreign counter-intelligence activities in support of Department of Defense components in coordination with the FBI in the United States and in coordination with the CIA overseas."

And present Section 4(e)(2)(iv) be renumbered as 4(e)(2)(v).

(5) Section 4(g) -- Section 4(g)(1) limits the FBI's counterintelligence activities to the "United States." Section 4(g)(2), however, allows the FBI to conduct foreign intelligence support activities at the request of Intelligence Community officials in the "United States and its territories." This distinction between the "United States" on one hand and the "United States and its territories" on the other was unintended.

Also Section 4(g)(1) does not acknowledge that on occasion the FBI may engage in counterintelligence activities overseas in coordination with the CIA. Because of this omission, it is unclear whether the FBI is authorized by E.O. 11905 to conduct operations outside the United States.

The FBI's jurisdiction to detect and prevent terrorism should be made explicit.

To conform to the definition in Section 2(a)(2), the term "counterintelligence" should read "foreign counter-intelligence."

Finally, the terms "subversion" and "other unlawful activities" should be deleted, and the term "clandestine intelligence activities" should be substituted for "espionage."

The subcommittee recommends that Section 4(g)(1) should be amended to read:

"Detect and prevent within the United States and its territories and, in coordination with the CIA subject to the approval of the DCI, outside the United States, sabotage, international terrorist activities, and clandestine intelligence activities by or on

foreign counterintelligence operations, including electronic surveillance, as are necessary or useful for such purposes."

Section 4(g)(4) should be amended by inserting the word "foreign" before the word "counterintelligence."

(6) Section 5's preamble -- The opening sentence of Section 5 gives the impression that only information about the capabilities and intentions of other governments is of interest in the foreign intelligence efforts of this country. Actually, entities other than governmental units engage in activities and have capabilities and intentions that are of comparable interest. For example, international terrorist groups, narcotics dealers, and political parties are of increasing concern in the field of national defense and foreign relations, and information about them, as well as about other governments, is essential to informed decision-making. The Order in various places makes clear that these entities are legitimate targets of foreign intelligence and counterintelligence activities.

The subcommittee recommends that the preamble to Section 5 be amended by deleting the words "other governments" in the first sentence and inserting in lieu thereof "foreign powers, organizations, or persons."

(7) Section 5(a)(6), for the purpose of requiring compliance with the various regulations and restrictions in Section 5, defines a foreign intelligence agency to be any agency (in addition to CIA, NSA, or DIA) "while engaged in the collection of foreign intelligence or counterintelligence." The intention was to include those elements of Defense, State, Treasury and other agencies which engage or might engage in intelligence activities. However, because collection is defined to include retention of information, the entire Department of State, for example, becomes a foreign intelligence agency under that definition.

To cure this problem the subcommittee recommends that Section 5(a)(6) be amended to read:

"(6) 'Foreign intelligence agency' means the Central Intelligence Agency, National Security Agency, and Defense Intelligence Agency; and further includes any other department or agency of the United States Government or component thereof while it is engaged in gathering foreign intelligence or foreign counterintelligence, but shall not include any such department, agency or component thereof to the extent that it is engaged in its authorized civil or criminal law enforcement functions; nor shall it include in any case the Federal Bureau of Investigation."

surveillance. This definition becomes operative in Section 5(b)(1) which prohibits physical surveillances with a list of exceptions. While the omission was unintentional, there is no exception where the subject of the surveillance has consented to the surveillance, as in the training and testing of operatives and in providing security to them in their missions. This omission can be cured by defining physical surveillance in terms of unconsented surveillance, as is done in the definition of electronic surveillance.[¶] In addition, the opening of a letter would fall within the definition of physical surveillance; however, the opening of mail in United States postal channels is governed by Section 5(b)(4) and the opening of other mail when directed against a United States person is governed by Section 5(b)(3). This potential conflict should be eliminated. Finally, physical surveillance, as defined, would include overhead reconnaissance, which was not intended and should be corrected.

The subcommittee recommends that Section 5(a)(8) be amended to read:

"(8) 'Physical surveillance' means an unconsented systematic and deliberate observation by any means on a continuing basis, except for overhead reconnaissance not directed at specific United States persons; or unconsented acquisition of a non-public oral communication by a person not a party thereto or visibly present thereat by any means not involving electronic surveillance."

(9) Section 5(b)(7) -- This paragraph prohibits the gathering, analysis, dissemination, or storage of non-publicly available information concerning the domestic activities of United States persons without their consent. Six exceptions to this prohibition are provided.

Traditionally all Federal agencies, including intelligence agencies, have forwarded to the Secret Service information relevant to Secret Service's protection of its protectees. However, no exception was made in this paragraph for such dissemination. This was unintentional.

The subcommittee recommends that the exception in subparagraph (v) be expanded to meet Secret Service's needs by amending it to read:

"(v) Information about a United States person who is reasonably believed to be acting on behalf of a foreign power or engaging in international terrorist or narcotics activities, or to present a danger to the safety of any person protected by the United States Secret Service."

(10) Section 5(c)(1) -- This paragraph states that nothing in Section 5 shall prohibit dissemination to law enforcement agencies of incidentally gathered information indicating involvement in activities in violation of law.

This paragraph was necessary because otherwise Section 5(b)(7) would have prohibited dissemination of information concerning domestic activities of United States persons unless it met one of the exceptions in that paragraph, and there was no general exception for information concerning criminal activities. Due to an oversight, however, the drafters failed to note that the preamble to Section 5 states that all references to law are to applicable "laws of the United States," and this term was intended to mean Federal laws. The result is that information incidentally acquired by a foreign intelligence agency which relates only to a violation of state law (e.g., murder) could not be disseminated to a local law enforcement agency unless it fell within one of the exceptions in Section 5(b)(7), which in many cases it would not.

To allow intelligence agencies to disseminate to local law enforcement agencies information about state and local crimes, incidentally acquired, which cannot be disseminated pursuant to Section 5(b)(7), the subcommittee recommends that Section 5(c)(1) be amended to read:

"(1) Lawful dissemination to the appropriate law enforcement agencies of incidentally gathered information indicating involvement in activities which may be in violation of Federal, state, or local laws or the laws of a foreign government."

II. Ambiguities

(1) Section 2(a) -- Throughout E.O. 11905 there are references to "terrorist activities," but the term is not defined. Moreover, regulations and procedures under the Order often use the same term -- again, usually without definition. In this increasingly important area, the subcommittee believes that the term should be defined.

The subcommittee recommends that a new definition should be added to Section 2(a) to read:

"(e) International Terrorist Activities
means violent acts or acts dangerous to human life, or threats of such acts, transcending national boundaries, which appear to be intended to further political, social, or economic goals by assassination, kidnapping, or intimidating or coercing the public or a government or to obtain widespread publicity for a group or its cause, and includes activities directly supportive of such acts."

(2) Section 5(e) -- Section 5(e)(1)(ii) prohibits intelligence agencies from "participat[ing] in or fund[ing] any law enforcement activity within the United States." Exception is made for "cooperation . . . for the purpose

of . . . preventing espionage or other criminal activity related to foreign intelligence or counterintelligence or . . . provision of specialized equipment or technical knowledge for use by any other Federal department or agency." Section 5(e)(2). This prohibition and its exceptions have raised probably more questions than any other provision in the Executive Order. While many of these questions have been resolved by interpretation, the subcommittee believes the language of Section 5(e) should be clarified.

The proposed change would make clear that outside the United States, intelligence agencies may, within the limits of their charters (both statutory and those within E.O. 11905), support Federal law enforcement agencies. It would also make clear that within the United States intelligence agencies may, within the limits of their charters, support Federal law enforcement agencies in investigating clandestine intelligence activities, international terrorism, and international narcotics trafficking. Finally, it would make clear that intelligence agencies may disseminate to law enforcement agencies information intentionally and lawfully collected for foreign intelligence and counterintelligence purposes. None of this represents a change from the Department of Justice's current interpretation of Section 5(e). It is nonetheless desirable that this interpretation be clearly reflected in the Order itself.

In addition, the subcommittee recommends one substantive change to Section 5(e)(2)(ii). This subparagraph presently makes an exception to the prohibition on participation in law enforcement for provision of specialized equipment or technical knowledge for use by any other Federal department or agency. The recent takeover of buildings in Washington demonstrated that there are instances when

technical knowledge or special equipment should be able to be made available to local law enforcement entities, as well as Federal agencies.

The subcommittee recommends that Section 5(e) be amended to read:

"(e) Assistance to Law Enforcement Authorities.

"(1) No foreign intelligence agency shall, except as expressly authorized by law (i) provide services, equipment, personnel or facilities to the Law Enforcement Assistance Administration or to State or local police organizations of the United States or (ii) within the United States participate in or fund any law enforcement activity.

"(2) These prohibitions shall not, however, preclude: (i) cooperation with appropriate law enforcement agencies for the purpose of protecting the personnel and facilities of the foreign intelligence agency, (ii) participation in law enforcement activities within the limit of the foreign intelligence agency's charter to investigate clandestine intelligence activities by foreign powers, international narcotics trafficking, or international terrorist activities,

(iii) the provision of specialized equipment or technical knowledge for use by any Federal department or agency, or when lives are endangered in support of local law enforcement activities, or (iv) the dissemination of information lawfully collected to any Federal or local law enforcement agency to enable it to investigate, prevent, or prosecute criminal activity."

(3) Section 6 -- In Section 6(b)(1), Inspectors General and General Counsels are to report to the IOB activities that raise questions of legality or propriety. There is no statement as to when such reports should be made.

Section 6(b)(2) is not clear as to what the periodic reports are to concern, and this should be clarified.

The reference to PFIAB, which has been abolished, should be deleted from Section 6(a)(1).

The organizational location of the IOB and the source of its funds is not clear in E.O. 11905 and should be made specific.

There is currently no requirement for the Attorney General to report to the IOB what action he has taken in response to its reports to him and there is a need, not reflected in the Order, for the Attorney General to keep the IOB abreast of legal decisions and interpretations affecting the Intelligence Community.

Therefore, the subcommittee recommends that Section 6(a) be amended by inserting the words "within the White House Office"

after the word "established"; that the second sentence of Section 6(a)(1) be deleted; that Section 6(b)(1) be amended by inserting "in a timely manner" after the word "transmit"; Section 6(b)(2) should be amended by deleting all after the word "Board" and inserting in lieu thereof "concerning what actions have been taken to comply with findings made by the Oversight Board or the Attorney General."; Section 6(d) should be amended by adding two new paragraphs to read:

"(3) Report to the Oversight Board in a timely fashion as to decisions made or actions taken in response to Oversight Board reports to the Attorney General.

"(4) Keep the Oversight Board informed as to legal opinions rendered affecting the legal duties of or restrictions on intelligence agencies or activities."; insert a new Section 6(f) to read

"(f) Compensation and allowances of the members of the Oversight Board and staff, together with expenses arising in connection with the work of the Oversight Board, shall be paid from the White House Office salaries and expense account and to the extent permitted by law from any corresponding appropriation which may be made in subsequent years."

III. Policy differences with E.O. 11905

(1) Section 4(a)(5) -- This paragraph requires senior officials of the Intelligence Community to report to the Attorney General "that information which relates to detection or prevention of possible violations of law by any person, including an employee of the senior official's department or agency." The Department of Justice has interpreted this provision as requiring reports whenever a department or agency has knowledge of a criminal or civil violation within the investigative or prosecutorial jurisdiction of the Department of Justice. The Central Intelligence Agency has never fully accepted this interpretation of the Order, and it reported this fact to the Intelligence Oversight Board in July, 1976. In August, 1976, the DCI requested John Marsh, Counsellor to the President, to seek relief from the Department of Justice interpretation or to have the Order amended. That letter specified a number of practical problems which the CIA believes to counsel against reports of crimes in certain situations. These problems were described by CIA as follows:

Applicants

Applicants for CIA employment, and other persons being considered for non-employment relationships with the CIA, are screened by the Office of Security. In the case of applicants for employment, the screening includes the administration of a polygraph examination, with follow-up questions often asked in order to clarify earlier responses or reactions. A good deal of personal information, some of it unfavorable, is disclosed during those screening procedures, and as a general rule that information is received in confidence. Were it otherwise -- that is, were a formal report to the Department of Justice required whenever the CIA received any information indicating possible violations of civil or criminal law, no matter how minor such violations -- these screening procedures would cease to be effective and the pool of applicants would be greatly reduced.

U.S. Citizen Sources

CIA contact officers often obtain valuable intelligence information on a voluntary basis from U.S. citizens, who in turn acquire that information in the course of their personal or business activities abroad. The assurances of absolute confidentiality that are customarily given to such sources would be foreclosed by the requirements of

Section 4(a)(5). In the absence of these assurances, much of the intelligence information now collected would never be imparted to CIA contact officers.

Sources Abroad

Clandestine service case officers develop close and confidential relationships with sources abroad based on mutual trust. From time to time, such sources make comments about their personal or business affairs that reveal possible violations of U.S. law. The case officer cannot effectively develop and maintain sources and play the role of informer at the same time.

Cover Situations

CIA employees are sometimes placed in cover positions in U.S. corporations abroad. In the course of their work, close relationships may be formed with other employees of the corporation who are not aware of the Agency employee's true status. The product of those relationships may be knowledge of irregular practices by the corporation or its employees. Such relationships would be jeopardized if CIA non-official cover employees had a mandatory role as Department of Justice informants.

Foreign Intelligence Service

Liaison arrangements between CIA and intelligence services of other countries may result in the receipt of

information which indicates possible violations of U.S. law by persons subject to U.S. jurisdiction. Foreign intelligence services require absolute assurances that information passed to us by them will not be used outside intelligence channels, and here again such assurances would be foreclosed by the requirements of Section 4(a)(5).

In all the circumstances mentioned above, the CIA's ability to function would be seriously impaired by a strict adherence to the reporting obligations imposed by Section 4(a)(5).

Option 1

Consequently, CIA recommends that Section 4(a)(5) should be deleted entirely, leaving 28 U.S.C. § 535(b) the sole mandatory crimes reporting requirement, and offers in justification the following:

Such a course of action is best calculated to ensure that CIA can fulfill its assigned mission, would keep CIA focused on foreign rather than domestic targets and still would adequately ensure prompt reporting to the Department of Justice or the Intelligence Oversight Board of any illegal or improper actions by the Agency as well as any violations of Federal criminal law by Agency employees.

E.O. 11905 was drafted in the wake of the Rockefeller Commission investigation of CIA activities within the United States to remedy two problems. The first was to guard against and prevent official Agency wrongdoing; the second was to protect the integrity of Government service by detecting illegal actions by Agency employees.

The Rockefeller Report, addressing this first concern, concluded after a detailed analysis of the facts that "the great majority of the CIA's domestic activities comply with its statutory authority," (Page 10) but that the Agency had engaged in a certain few activities which were beyond its charter responsibilities. The problem of official abuses was dealt with in gross by setting up the organizational structures detailed in Sections 3 and 6 of this Order and in fine by a rigorous definition of the duties of the Agency (Section 4(b)) and a clear enumeration of restrictions on intelligence activities (Section 5).

The Rockefeller Report also addressed the second concern -- violations of law by Agency employees. It noted that "the Department of Justice had abdicated its statutory duties and placed on the Director of Central Intelligence the responsibility for investigating criminal

conduct and making the prosecutorial decision -- clearly law enforcement powers." (Page 75) To cure the problem, the Report recommended that the Department of Justice and the CIA establish written guidelines for the handling of reports of criminal violations by employees of the Agency or relating to its affairs. (Page 82) Steps to implement this recommendation have been taken. The 1954 agreement between CIA and the Department was invalidated, interim reporting procedures were established and work on a formal Draft Memorandum of Understanding to be signed by the Attorney General was begun and is nearing completion. In this regard, however, it is only fair to note that even during the twenty-year period of the agreement, all but a handful of routine cases were discussed with the Department and the Rockefeller Report itself, after deploring the existence of the 1954 agreement between the CIA and the Department of Justice, went on to say: "There is, however, no evidence that these powers were ever abused by the Agency." (Page 75). In sum, neither the requirement to protect against official abuse nor the need to guard against malfeasance or misfeasance by Government employees justifies promulgation of 4(a)(5).

Not only does 4(a)(5) in both its present language and as presented in Option 2 appear to be unnecessary as a corrective to past abuses, it is harmful to intelligence and to public perception of the Intelligence Community. The harm to intelligence derives from the fact that the Agency's relationship with its sources is a fragile and precarious one. Individuals who cooperate with the Agency would often be in extreme danger if such collaboration were known, businesses which cooperate may face reprisals if such cooperation were discovered. Against this backdrop of danger and fear, only the firmest assurance that the Agency can and will protect intelligence sources allows for continued recruitments and continued collaboration.

It is no secret that access, for example to corporations or corporate officials, on a continuing basis not only gives us access to valuable foreign intelligence, but also to corporation secrets and proprietary information which may reveal violations of law. Should CIA be viewed as an arm of U.S. regulatory or law enforcement agencies, such access would be summarily terminated and much of the intelligence information now collected by these means would become unavailable to the U.S. Government.

Even more significant to the Agency are cases in which corporations may provide operational support or nonofficial cover for CIA officers. Such an officer may easily become aware of irregular practices of the corporation or its employees. It is most unlikely that such corporations would continue to welcome in nonofficial cover positions CIA employees who were required to act, in effect, as Department of Justice, IRS or SEC informants. Further, if the nonofficial cover employee were required to testify as a result of information provided to such agencies, his usefulness to the CIA in any cover operation would be destroyed.

Beyond these specific problems is the more general concern that Section 4(a)(5) represents a dangerous narrowing of the gap between intelligence and law enforcement. It would be ironic, indeed, if an investigation triggered by concern about CIA's domestic activities led to reporting requirements which caused the Agency to appear to intrude even more than before into the lives of American citizens.

The Rockefeller Report itself notes that the prohibition in the National Security Act of 1947 "that the Agency shall have no police, subpoena, law enforcement power, or internal-security functions" was imposed because "Congress

sought to assure the American public that it was not establishing a secret police which would threaten the civil liberties of Americans." (Page 10-11) In sum, both the CIA and National Security Acts were designed to keep CIA essentially pointed toward foreign areas and away from domestic involvement to ensure that mechanisms used to procure foreign intelligence were not used to procure information about the lives, beliefs or actions of U.S. citizens. The Acts also sought to ensure that the Agency, an arm of the foreign policy apparatus, did not also become the eyes and ears of the law enforcement apparatus.

It seems, moreover, that the major thrust of E.O. 11905, for example, Sections 5(e)(1) and 5(b)(1), is to generally prohibit a foreign intelligence agency from intentionally collecting information for domestic prosecutorial purposes. A mandatory requirement that intelligence agencies report criminal violations raises the implication that at a minimum such agencies are to alert their personnel to monitor files to detect such violations, and possibly to actually collect such information. This may represent a degree of cooperation between foreign intelligence and law enforcement agencies which would be improper. If the Agency is to follow the spirit and letter of the National

Security Act, and indeed of Section 5(e)(1) of the Order, it cannot be forced to operate or seem to operate as an extension of law enforcement agencies in the U.S.

The ^{Agency} / appreciates that the Order is not intended to erect a wall of complete separation between the product of intelligence activities and domestic law enforcement. Section 5(c)(1) of the Order allows "dissemination to the appropriate law enforcement agencies of incidentally gathered information indicating involvement in activities which may be in violation of law" and the Department of Justice recommends a broadening of this provision to include violations of state and foreign law. There is, however, a significant difference between 4(a)(5) and 5(c)(1). The one, by its mandatory tone, turns the Agency into a constituent part of the police informant net, the other, permissive in character, recognizes the primacy of the Agency's intelligence functions and also recognizes that the statutory responsibility of the Director of Central Intelligence (50 U.S.C. 403(g) and Executive Order 11905, Section 3(d)(vii)) provides authority, within certain limits, for him to withhold information from law enforcement officials if he believes its disclosure would threaten the security of intelligence sources or methods.

It is appreciated that Option 2 is a substantial improvement over the present language of 4(a)(5), however, CIA submits that if the eight categories of criminal violations are important enough to warrant a special mandatory reporting requirement, then such requirement ought to be the subject of a separate Executive Order and, as with 28 U.S.C. 535(b), the heads of all executive branch department and agencies should be required to so report.

Agency,
The /of course, would not like to see all U.S. agencies and all U.S. Government employees cast in the role of informers, but the Agency is even more doubtful about the wisdom of casting foreign intelligence agencies in such a "big brother" role. Once it is realized that foreign intelligence agencies and foreign intelligence agencies alone are to be police informants, then such agencies will be regarded less as a bulwark against foreign enemies and more as a threat to American privacy. E.O. 11905 has, as its purpose, improvement in the quality of intelligence needed for national security, clarification of the responsibilities of intelligence agencies and departments, and establishment of effective oversight to assure compliance of law in the management and direction of foreign intelligence. The Agency does not believe that these goals are advanced when foreign intelligence agencies are singled out and made to function as police informants.

Option 2

The Department of Justice disagrees with CIA's recommendation and analysis, although Justice believes that the present Section 4(a)(5) should be amended to narrow its present scope, but does not believe as a policy matter, that the requirements of 28 U.S.C. § 535(b) are sufficient for the intelligence agencies.

Addressing CIA's philosophical objections first, the CIA suggests that intelligence agencies should not be singled out as the only agencies with a mandatory reporting requirement broader than 28 U.S.C. § 535(b). Yet the primary motivating factor behind E.O. 11905, and especially the restrictions in Section 5, was to single out the Intelligence Community for special treatment because of perceived past abuses. No other agencies operate under the restrictions of Section 5; no other agencies have Executive charters which specify the exclusive limits of their functions and responsibilities.

One of the so-called abuses of intelligence agencies was their alleged failure to report criminal violations to the Department of Justice. With respect to CIA, the Rockefeller Commission concluded that it was a violation of CIA's statutory charter to be given the power to decide what crimes should be investigated. Specifically, it faulted CIA for not being forthcoming with respect to information it possessed concerning the Watergate cover-up. Rockefeller Commission Report at 199-202.

To cure the problem which it perceived, the Commission recommended:

"The Department of Justice and the CIA should establish written guidelines for the handling of reports of criminal violations by employees of the Agency or relating to its affairs. These guidelines should require that the criminal investigation and the decision whether to prosecute be made by the Department of Justice, after consideration of Agency views regarding the impact of prosecution on the national security. . . ." Rockefeller Commission Report at 82. (Emphasis supplied)

This recommendation was the origin of Section 4(a)(5). The Ford White House made a conscious decision, however, to broaden in two ways the reporting requirement suggested by the Rockefeller Commission. First, it expanded the reporting to include not just violations by employees of the CIA or relating to its affairs, but also violations by any other person. Second, it expanded the reporting requirement to all intelligence agencies. The important point for

present purposes is that the intent was to levy a requirement on intelligence agencies to report to the Attorney General "any information they may obtain which relates to the commission of federal crimes." See Executive Order Annotations, from Jack Marsh, dated March 10, 1976.

Thus, the partial answer to CIA's question why intelligence agencies should be singled out is that, because of the perception of recent history, there was a felt need to place special restrictions and requirements on intelligence agencies. Another part of the answer is the unusual nature of intelligence work; that is, that it requires a large degree of secrecy to be effective. The basis for singling out the intelligence agencies for special requirements is that other agencies will in all likelihood report criminal violations to the Justice Department, because they have no countervailing motive not to. On the other hand, CIA has a vital interest in protecting its sources and methods, and if reporting a crime to the Department of

Justice might result in an investigation or prosecution, those sources and methods might be compromised. CIA might well conclude that the protection of its sources and methods was more important than investigation or prosecution, and the crime would not be reported.

The Rockefeller Commission carefully considered the competing considerations and concluded that the ultimate decision whether to investigate or prosecute should be left not to CIA, but to the Department of Justice -- after full consideration of the CIA's views as to the effect an investigation or prosecution would have on the national security. Yet that ultimate decision cannot be made if the CIA will not in fact report crimes to the Department of Justice in the first instance.

CIA questions why the reporting requirement must be broader than that under 28 U.S.C. §535(b), which is limited to reporting crimes under title 18 by Government employees. The answer to this question is essentially the same as the answer above to why intelligence agencies are singled out for treatment; that is, generally only

intelligence agencies have a legitimate countervailing interest in not reporting crimes by other persons or other crimes by employees. The limited scope of 28 U.S.C. § 535(b) is explained by the fact that its primary purpose was to insure that agencies would report crimes by their employees which they might not otherwise report because it would reflect badly on the agencies' management. Virtually all such crimes are found in title 18 and, therefore, are covered by § 535(b).

Finally, CIA suggests that the reporting requirement would involve intelligence agencies in the active collection of information for law enforcement purposes, and that this is contrary to the spirit of the National Security Act and Section 5(e) of E.O. 11905. The Department of Justice disagrees. The reporting requirement is just that, nothing more. If an intelligence agency incidentally acquires evidence or becomes cognizant of a serious crime, it should report it. There is no obligation or suggestion that intelligence agencies make any file checks, ask any questions to find evidence of a crime, or investigate any activity to determine if a crime has been committed (other than any investigation of the facts the Inspector General might make of employee misconduct or of the law that the General Counsel might make to determine if

questionable conduct is criminally unlawful). There is no affirmative obligation to detect and investigate criminal activities.

In addition to these objections, CIA has raised certain practical problems. Some of these the Department of Justice believes can be alleviated in a new Section 4(a)(5) which would be narrower in its scope than the present section by requiring an agency to report only those crimes serious enough to require case-by-case determinations and exclude those crimes which it can be fairly said would never be prosecuted given the importance of protecting intelligence sources and methods.

Job Applicants -- CIA suggests that because job applicants are subjected to a polygraph examination which with some regularity results in the admission of almost invariably minor criminal acts, a requirement to report such information would result in a substantial loss of potential job applicants. Under a revised Section 4(a)(5) listing serious crimes, it would appear that this problem would be virtually eliminated. To the extent a reporting requirement of identified serious crimes would impact on CIA's pool of applicants, such impact would appear to be a benefit, not a hindrance. Even under the

present Section 4(a)(5) NSA has been reporting to the Department of Justice crimes identified in polygraphs of job applicants with no apparent effect on their applicant pool.*/

Cooperating Intelligence Sources -- The CIA states that in the course of CIA's relationship with such sources evidence of crimes by them may come to its attention.

*/ NSA reports periodically to the Department by listing the crimes identified without identifying the person involved. If the Department believes the crime worthy of investigation, it then requests the additional information in NSA's possession. This system has apparently been to the satisfaction of both NSA and the Department.

If CIA were required to report such crimes to the Department of Justice, CIA would be hampered in obtaining such sources. First, the Department of Justice notes that the reporting requirement has been on the record for a year, and unless CIA has affirmatively assured its sources that it does not comply with this requirement, CIA has apparently not been hampered thus far. Even if CIA complied with the reporting requirement, CIA's sources would be unaware of any particular report / unless the Department of Justice did in fact investigate or prosecute, and even if Justice did investigate and prosecute it is entirely possible that the original source of the information would not be revealed. Obviously the Department of Justice would be sensitive to CIA's concerns in determining whether or not to investigate. Finally, to the extent the crimes were minor they would not be included in an amended reporting requirement, and to the extent they were serious crimes, the Department of Justice believes that the decision whether or not to investigate or prosecute should not be left to CIA alone.

Cover Relationships -- CIA states that its employees who require cover in private commercial enterprises might become aware of corporate crimes. Again, Section 4(a)(5)'s reporting requirement has been public knowledge for over a year, and it has not apparently impeded CIA's ability to

utilize private commercial enterprises for cover purposes. And as was discussed above with respect to cooperating sources, the commercial enterprises would not be aware if crimes were reported unless the Department of Justice decided to investigate, and even then the source of the information could normally be protected.

Foreign Intelligence Services It would be a rare case indeed where a foreign intelligence service would report information meeting a revised Section 4(a)(5) standard, which the Department of Justice would utilize in a criminal prosecution. However, in the extreme case of an assassination within this country, for example, information which would lead to the apprehension of the perpetrators obviously should be reported to the Department of Justice. Investigations and even prosecutions need not disclose the source of such evidence, so that the assurances given to foreign services could be maintained. Moreover, there is little doubt that foreign services have utilized and will utilize outside intelligence channels, information we have given them, when they find it desirable and it can be done in a manner to protect the source.

In conclusion, the Department of Justice believes that at least with respect to certain classes of serious crimes the CIA and other intelligence agencies should not be left with the responsibility or opportunity to exercise a law enforcement function -- to wit, the final determination whether a crime should be investigated or prosecuted. The Department of Justice recommends that Section 4(a)(5) be amended to read: */

"Report to the Attorney General that information required by 28 U.S.C. § 535(b) and in addition any information, however acquired, evidencing violations of Federal law in the following classes of criminal cases:

- (i) violations of law endangering a person's physical safety;
- (ii) violations of 18 U.S.C. §§ 241, 242, 245;
- (iii) violations of law affecting the integrity of government (e.g., bribery, serious conflicts of interest, serious violations of election laws, perjury, obstruction of justice, misprision of a felony);

- 38 -

*/ The Department of State concurs in this recommendation.

(iv) violations of law involving espionage, sabotage, or terrorism;

(v) violations of law involving willful disclosures of classified information intended to reach the public at large or a foreign power;

(vi) violations of law involving fraud on or theft from the Government involving money or things of value over \$10,000;

(vii) violations of chapter 119, title 18, United States Code; and

(viii) violations of law by foreign intelligence services in the United States."

Option 3

Section 4(a)(5) be amended to read:

"Report to the Attorney General that information required by 28 U.S.C. § 535(b) and in addition any information, however acquired, evidencing violations of Federal law in the following classes of criminal cases when such violations are committed by U.S. or foreign Intelligence Agency operatives:

(i) violations of law endangering a person's physical safety;

(ii) violations of 18 U.S.C. §§ 241, 242, 245;

(iii) violations of law affecting the integrity of government (e.g., bribery, serious conflicts of interest, serious violations of election laws, perjury, obstruction of justice, misprision of a felony);

(iv) violations of law involving espionage, sabotage, or terrorism;

(v) violations of law involving willful disclosures of classified information intended to reach the public at large or a foreign power;

(vi) violations of law involving fraud on or theft from the Government involving money or things of value over \$10,000;

(vii) violations of chapter 119, title 18, United State Code; and

(viii) violations of law by foreign intelligence services in the United States."

CIA prefers this option over option 2 on the following basis:

This option would extend the reporting requirement levied on intelligence agencies beyond that required of other Government agencies to cover reporting violations by the intelligence services of other nations and also violations by U.S. intelligence operatives. Although such reporting could create severe security problems for U.S. intelligence agencies, this option may represent a proper balancing of intelligence and prosecutive interests. By essentially limiting the reporting requirement to people who are extensions of intelligence and eliminating the need to report on third parties whose actions are unrelated to intelligence, two CIA objectives are achieved. First, those individuals or corporations which are willing to collaborate with the U.S. Government for certain limited purposes will be encouraged to do so and second, the citizenry at large will not begin to identify U.S. foreign intelligence agencies as part of a domestic police informant network. Nevertheless, CIA believes that Option 1 is preferable to this option.

The Department of Justice prefers this option over Option 1 because it includes those cases which intelligence agencies are most likely to acquire information about and

which are the most serious in terms of possibly discrediting intelligence agencies if not reported. Nevertheless, the Department of Justice believes that Option 2 is preferable to this option.

Option 4

The Department of Defense disagrees with Options 1-3, but agrees with the need to limit Section 4(a)(5). Defense believes, however, that this limitation need not be spelled out in the Order itself; instead the details of the threshold reporting requirements should be left to separate understandings with the Justice Department, and that Section 4(a)(5) be amended to provide for this possibility.

The Department of Defense, however, concurs with CIA that Option 2 is not appropriate to the extent that it goes beyond Option 3.

Therefore, the Department of Defense recommends that Section 4(a)(5) be amended to read:

"(5) Report to the Attorney General criminal violations of Federal law by any person, including an employee of the senior official's department or agency, pursuant to guidelines adopted by the Attorney General."

The Department of Justice is not fundamentally opposed to this option, but it notes that this option rests substantial discretion in the Attorney General. On the one hand, this could theoretically allow agreements of the nature condemned by the Rockefeller Commission, and it has been the Department of Justice's interpretation of the current Section 4(a)(5) to prohibit such agreements, because the Department of Justice was equally at fault in abdicating its responsibilities before the Executive Order, as intelligence agencies were in improperly extending their responsibilities to include a determination whether a criminal investigation should go forward. If this option is adopted, it would be the intention of the Department of Justice to require by guidelines the reporting outlined in Option 2. Therefore, the fundamental issue of whether Option's 2 requirements are to be put into effect must be decided under this option as well.

(2) Section 4(h) -- This would be a new section. At the time of E.O. 11905's issuance the inclusion of the Drug Enforcement Administration in the charter section

of the Order was considered, but rejected, on the basis that its intelligence activities were only ancillary to its law enforcement functions. This perception was not totally accurate. In fact, DEA is pursuant to prior USIB mandates the lead agency for narcotics intelligence throughout the Executive Branch. As such it has an intelligence collection, production, dissemination, and requirements-setting function separate from its enforcement function. Therefore, the subcommittee recommends that DEA be represented among the intelligence agencies which have charters in Section 4 of E.O. 11905.

The subcommittee recommends that a new Section 4(h) be added to E.O. 11905 to read:

"(h) The Drug Enforcement Administration. Under the supervision of the Attorney General and pursuant to such regulations as the Attorney General may establish, the Administrator of DEA shall:

(1) Collect, produce, and disseminate intelligence on the foreign and domestic aspects of narcotics production and trafficking in coordination with other departments and agencies with responsibilities in any of these areas.

(2) Participate with the Department of State in the overt collection of general foreign economic, agricultural, and political information relating to narcotics activities.

(3) Coordinate with the Director of Central Intelligence to ensure that the United States foreign narcotics intelligence activities are consistent with the United States foreign intelligence policy."

And a new Section 2(b)(10) to read:

"(10) Intelligence element of the Drug Enforcement Administration."

And in Section 4(a), after "ERDA" insert ", DEA".

(3) Section 5(b)(6) -- This section prohibits intelligence agencies from the infiltration or undisclosed participation within the United States in any organization "for the purpose of reporting on . . . its . . . members," except for organizations believed to be acting on behalf of a foreign power and composed primarily of non-United States persons. This prohibition raises a problem where CIA participates without disclosing its identity in an organization in order to identify those members of the organization who may be useful to contact and recruit or debrief.

When the member is in fact contacted, usually not in the context of the organization, CIA will disclose its identity, but prior to this time there will be certain reporting concerning the member's travel, acquaintances, etc., to determine the desirability of making the contact. This appears to be prohibited by the present section, and the Executive Order annotations, which explain the provision as barring infiltration "for the purpose of collecting foreign intelligence or counterintelligence," reinforces this interpretation.

While there is a certain potential for abuse in allowing CIA to report on the activities of members of domestic groups for purposes of determining the desirability of recruiting or debriefing them, CIA believes this source of information is extremely valuable, and notes that the Order provides a similar exception from the prohibition on the collection of information.

Therefore, the subcommittee recommends that Section 5(b)(6) be amended by adding at its end:

"and except reporting on members of organizations who are reasonably believed to be potential sources or contacts, but only for the purpose of determining whether the person is a desirable source or contact."

(5) Section 7 -- Section 7 requires that all members of the Executive Branch and its contractors given access to information containing sources and methods of intelligence shall, as a condition of access, sign an agreement not to disclose that information to unauthorized persons. This Section is being violated by a number of departments and agencies. Some simply have not yet undertaken to draft such an agreement; some have not required those persons who already had access at the time of the Executive Order to undertake such an agreement; others have believed a secrecy "oath" was sufficient; and others have exempted certain officials from the requirement of undertaking a Secrecy agreement on the grounds that it would be demeaning.

The subcommittee is not convinced of the need for a Secrecy Agreement at all. Only on rare occasions will its provisions be able to be enforced judicially.

The subcommittee believes the present Section 7 should not be retained. It is overinclusive in that it requires a Secrecy Agreement with respect to information which is not classified, which is probably not judicially enforceable; and it is underinclusive in that it is limited to information related to sources and methods. Finally, the widespread violation of this Section demonstrates that as presently drafted it is inappropriate.

The subcommittee, therefore, recommends that Section 7 be deleted from the Order altogether. ^{*/} The subcommittee further recommends that the group reviewing E.O. 11652 should consider the desirability of an improved Secrecy Agreement for possible inclusion in a revised E.O. 11652, which would be a more rational placement for such requirement.

*/ The Department of Defense dissents from this recommendation, believing that pending the improvement of the Agreement and its inclusion in an amended E.O. 11652, the current provision should remain.

~~SECRET~~

June 1, 1977

SUBCOMMITTEE REPORT TO THE SCC

Executive Summary

Re: Lack of Authority for Electronic Surveillance Abroad and Physical Searches within and without the United States.

The attached report to the SCC is made pursuant to PRM/NSC-11 by the Subcommittee acting under the direction of the Attorney General.

The report addresses the problem caused by the lack of any Presidential delegation to the intelligence agencies or the Attorney General to engage in foreign intelligence physical searches in the United States and foreign intelligence physical searches and electronic surveillances directed against United States persons overseas.

The Subcommittee concludes that legislation should be sought authorizing these activities, but pending the enactment of such legislation, the President should delegate authority to the Attorney General to approve electronic surveillance abroad directed against United States persons in the same manner as he does for electronic surveillances in the United States. In addition, the Subcommittee recommends that the President delegate the authority to the Attorney General to approve and adopt procedures governing foreign intelligence physical searches at home and directed against United States persons abroad in two limited circumstances: (1) where the property to be searched is in the custody of the United States or its agents; and (2) where the property is on the premises of a foreign power to which the United States or its agents have lawful access. No authority for breaking and entering of any real property is to be delegated.

Attachment

CLASSIFIED BY John M. Harmon, Acting Assistant Attorney General, Office of Legal Counsel, Department of Justice; XGDS, Cat. 2; DATE OF DECLASSIFICATION: Indefinite.

~~SECRET~~

~~SECRET~~

June 1, 1977

REPORT TO THE SPECIAL COORDINATION COMMITTEE

Re: Lack of Authority for Electronic Surveillance
Abroad and Physical Searches within and without
the United States.

This report is submitted to the SCC by the SCC Subcommittee acting under the direction of the Attorney General pursuant to PRM/NSC-11.

Appendix A to this report is an opinion of the Acting Assistant Attorney General, Office of Legal Counsel, to the effect that while the President has the constitutional power to authorize warrantless physical searches of foreign powers and their agents in the United States and warrantless physical searches and electronic surveillance of United States persons abroad who are agents of foreign powers, the President has never, except in PD/NSC-9 and NSCID-6, generally authorized such searches and surveillances. As there has been no delegation of authority from the President, the Attorney General cannot approve such searches and surveillances. Moreover, the Attorney General is of the view that the previously issued Attorney General procedures for such searches and surveillances in exigent circumstances should be suspended pending a delegation of Presidential authority. This means that at

CLASSIFIED BY John M. Harmon, Acting Assistant Attorney General, Office of Legal Counsel, Department of Justice; XGDS, Cat. 2; DATE OF DECLASSIFICATION: Indefinite.

~~SECRET~~

~~SECRET~~

present such searches and surveillances cannot be conducted without either an extraordinary, ad hoc judicial warrant or specific Presidential approval.

It may appear strange that the President would have prohibited electronic surveillance and physical searches directed against United States persons abroad except in accordance with procedures approved by the Attorney General unless the President believed that such procedures could in fact be approved. Doubtless in February 1976 it was generally believed that CIA had the authority to engage in such searches, so long as they were conducted in accordance with procedures which assured their legality. The law in this area, however, has developed substantially since February 1976. In March of that year a court held that warrants were required for national security electronic surveillances abroad, unless the target was an agent of a foreign power. See Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144 (D.D.C. 1976). In May the D.C. Circuit focused for the first time on the need for explicit Presidential delegations. See United States v. Ehrlichmann, ___ F.2d ___ (D.C. Cir. 1976). While it came as no surprise to learn that the FBI could not make break-ins without Presidential authorization, it was now realized that the FBI could not make any foreign

-2-

~~SECRET~~

~~SECRET~~

intelligence physical search, which would in a criminal context require a warrant, without a Presidential authorization.

The question whether CIA already had such authorization was not clear, and because of a lack of requests for overseas searches and surveillances requiring a determination of that question, the issue was not in fact resolved until earlier this year.

The long-term solution to the problem raised by this lack of authority should be legislation, which would require warrants for physical searches within the United States along the lines of the present electronic surveillance legislation, and either warrants or statutory authorization with civil liberties safeguards for electronic surveillance and physical searches abroad. And the Administration has already committed itself to legislation in these areas. In the overseas area the problem of American participation with foreign agencies in law enforcement activities could also be addressed.

For the short term, the alternatives are (1) to seek Presidential authorization patterned after the President's February 3, 1977 memorandum regarding electronic surveillance within the United States; (2) to seek Presidential authorization on a case-by-case basis; (3) to seek extraordinary judicial warrants; or (4) to refrain from all physical searches in the

-3-

~~SECRET~~

~~SECRET~~

foreign intelligence and counterintelligence areas in the United States and all physical searches and electronic surveillances (not within NSCID-6 and PD/NSC-9) directed against United States persons abroad until authorizing legislation is enacted.

The CIA and FBI believe option (2) calling for specific Presidential authorization on a case-by-case basis to be generally unworkable because the cases that have arisen are routine and are not of a type that would merit the President's attention. The CIA believes option (3), extraordinary judicial warrants, is unacceptable because in the normal case the danger to the security of sensitive sources and methods posed by going to a random judge with no mandated security procedures (similar to those in the proposed electronic surveillance bill) would outweigh the need to make the particular search or surveillance. In addition, there are legal questions as to the ability of courts to grant warrants for such searches and surveillance absent statute. Both CIA and FBI find option (4), which would preclude all such searches and surveillances until legislation is enacted, to be unacceptable because valuable foreign intelligence is being lost and it is expected that legislation could not be obtained in less than two years.

-4-

~~SECRET~~

~~SECRET~~

In the past year, there have been several situations in which a physical search was desired where the matter to be searched was in the custody of the United States or its agents.

25X1

It is these two classes of cases where a continuing need for search authority exists before legislation can be obtained. Moreover, these searches are not the intrusive breaking and entering searches which have raised the gravest questions.^{*/} Rather these searches are more akin to the "technical trespasses," which Judges Leventhal and Merhige appeared willing to accept in United States v. Ehrlichman, ___ F.2d ___ (D.C. Cir. 1976) (concurring opinion).

^{*/} There has been no request by any agency for a physical search involving breaking and entering real property, and while the need for such a search might arise in the future, its rarity plus the extraordinary nature of the search suggests that such searches be approved only by the President himself or by an ad hoc judicial warrant.

-5-

~~SECRET~~

~~SECRET~~

The Subcommittee, therefore, recommends that the President direct the SCC Subcommittee to draft legislation by July 31, 1977, covering physical searches at home and abroad and electronic surveillance abroad. In the interim the Subcommittee recommends (1) that the President issue a memorandum to cover overseas surveillance in the limited circumstances and under the same procedures outlined in his February 3 memorandum to the Attorney General relating to electronic surveillance in the United States; and (2) that the President delegate to the Attorney General the power to approve or adopt procedures approving warrantless physical searches where either the searcher is consensually on the premises of a foreign power, but not necessarily permitted access to a particular location or object thereon, or the personal property to be searched is in the lawful custody of the United States or its agent. In all other circumstances either specific Presidential approval or a judicial warrant will be required, except that in emergency situations where a life is in danger other searches may be made.

A draft Presidential Directive is attached which would accomplish this end. See Appendix B.

Attachment

-6-

~~SECRET~~

~~SECRET~~

June 1, 1977

MEMORANDUM

Re: Lack of authority for electronic surveillance
abroad and physical searches within and
without the United States.

In criminal cases in the United States a prior judicial warrant is normally required to authorize either a physical search or an electronic surveillance without the consent of a party. Certain courts have, however, upheld warrantless electronic surveillance conducted within the United States pursuant to the President's constitutional power to gather foreign intelligence. See United States v. Butenko, 494 F.2d 593 (3d Cir. 1974); United States v. Brown, 484 F.2d 418 (5th Cir. 1973). This exception to the warrant requirement has been narrowly construed to

XGDS, Cat. 2; DATE OF DECLASSIFICATION: Indefinite

~~SECRET~~

allow only the targeting of persons who are agents of or collaborators with a foreign power. See Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975). There is only one district court decision directly relating to electronic surveillance of United States persons abroad, but its holding was likewise that a prior judicial warrant is required, except in exigent circumstances, unless the surveillance is of an agent of a foreign power pursuant to the President's constitutional authority. See Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144 (D.D.C. 1976). While the Department of Justice has not conceded the validity of that holding -- requiring warrants overseas for non-foreign intelligence electronic surveillances directed against United States persons -- the Berlin Democratic Club decision is consistent with prior decisions, see Powell v. Zuckert, 366 F.2d 634 (D.C. Cir. 1966), and pending further legal developments the Department of Justice is proceeding in accordance with the decision.

There are no court cases explicitly recognizing warrantless physical searches of agents of foreign powers pursuant to the President's constitutional power to gather foreign intelligence. The only case to speak directly to physical entry for foreign intelligence purposes, other than to plant a bug, is United States v. Ehrlichman, 376 F. Supp. 29, 32-34

~~SECRET~~

(D.D.C. 1974), aff'd, ____ F.2d ____ (D.C. Cir. 1976). In the district court Judge Gesell held that the President did not have the power to authorize a warrantless search of an American citizen "whenever the President determines that an American citizen, personally innocent of wrongdoing, has in his possession information that may touch upon foreign policy concerns," 376 F. Supp. at 33, or, in the alternative, even if the President did possess such power, he had not authorized the break-in in that case. Judge Gesell acknowledged, however, the possibility of Presidential power "under the most exigent circumstances." Id. While this case is often cited for the proposition that warrantless physical searches for foreign intelligence are unconstitutional, its holding does not go that far. Indeed, on this point its holding is consistent with Zweibon v. Mitchell, supra; that is, unless the target of the search is an agent or collaborator with a foreign power, a warrant is required.

On appeal the Department of Justice filed an amicus brief stating:

It is and has long been the Department's view that warrantless physical entries into private premises are justified under the proper circumstances when related to foreign espionage or intelligence.

Subsequently, the Office of Legal Counsel of the Department of Justice reviewed the existing case law and statutes and determined that, notwithstanding the district court's decision, "given a 'foreign intelligence' exception to normal warrant requirements, physical entries are permissible or not according to their 'reasonableness,' and are not categorically excluded from the exception."

It is, therefore, my opinion that the President does have the constitutional power to authorize warrantless electronic surveillance and warrantless physical searches of foreign powers or their agents.

The circuit court in Ehrlichman affirmed the district court decision on the basis that whether or not there was an exception to the warrant requirement for physical searches for foreign intelligence conducted pursuant to the President's constitutional powers, neither the President nor the Attorney General had authorized the Fielding break-in and hence the search could not be justified on the basis of whatever constitutional power the President might have.

The President, by memorandum dated February 3, 1977, delegated to the Attorney General his authority and authorized

~~SECRET~~

~~SECRET~~

the Attorney General to approve warrantless electronic surveillance, and the necessary intrusion to effect the surveillance, within the United States directed against foreign powers or their agents, according to the procedures delineated in the memorandum. It is pursuant to this authority that the Attorney General has approved warrantless electronic surveillances within the United States. The President has never delegated to the Attorney General the authority, or authorized him to approve electronic surveillances abroad or physical searches either within or without the United States.^{*/} Therefore, at the present time the Attorney General has no authority to approve such surveillances or searches.

Section 5(b)(2) of E.O. 11905 prohibits intelligence agencies from conducting electronic surveillance of communications to or from the United States or directed at United States persons abroad except pursuant to procedures approved by the Attorney General. Similarly, Section 5(b)(3) of E.O. 11905 prohibits intelligence agencies from conducting unconsented physical searches abroad except pursuant to procedures approved by the Attorney General. It has been argued that these exceptions to the prohibitions constitute a positive authorization to the Attorney General, but given the statement in the preamble to Section 5 that "This Section

^{*/} One narrow exception is PD/NSC-9 which authorizes the Attorney General to approve warrantless electronic surveillance and mail openings directed against United States persons in Berlin.

~~SECRET~~

of this Order does not authorize any activity not previously authorized . . . , " I do not believe the exceptions to the prohibitions can be read as positive authorizations to the Attorney General to approve electronic surveillance or physical searches abroad directed against United States persons.

The question has also been raised whether express authorization from the President is required for the Attorney General to approve warrantless surveillance or searches. On the basis of the court's statement in United States v. Ehrlichman, ___ F.2d ___ (D.C. Cir. 1976) that the Attorney General is the President's "alter ego for these matters," it can be argued that no express delegation or authorization is required. Support for this proposition is also found in In re Neagle, 135 U.S. 1 (1890), where an order of the Attorney General absent Presidential authorization or delegation was found to be a valid exercise of the President's constitutional powers. Nevertheless, in the particular area of foreign intelligence searches and surveillance, where Presidents have traditionally utilized an explicit delegation or authorization to the Attorney General to approve electronic surveillance in the United States, ^{*/} it is singularly inappropriate for

*/ See also PD/NSC-9.

~~SECRET~~

the Attorney General to arrogate to himself the full powers of the President to approve warrantless searches absent an explicit Presidential directive to that effect. See also Department of Justice Report Concerning its Investigations and Prosecutorial Decisions with respect to Central Intelligence Agency Mail Opening Activities in the United States 35-39 (1977).

I read NSCID-6 as a specific authorization for the appropriate agencies to engage in communications intelligence activities, including by implication the targeting of United States persons. However, if activities undertaken pursuant to NSCID-6 do target United States persons or communications to or from the United States, these activities must be in conformity with procedures approved by the Attorney General. See Section 5(b)(2), E.O. 11905. Therefore, it is my opinion that the Attorney General can lawfully approve, under the standards in the various procedures, the targeting of a United States person by communications intelligence activities, because these activities have been specifically authorized by the President in NSCID-6.

~~SECRET~~

Other electronic surveillance ~~inside~~ the United States and physical searches within or without the United States, however, have not, to my knowledge, ever been specifically authorized by the President.*/ Therefore, neither the agencies involved nor the Attorney General have been authorized by the President to invoke his constitutional power to utilize a warrantless search in these situations to gather foreign intelligence from foreign agents.

Consequently, at the present time I believe that before a United States person can be the target of a physical search within the United States or abroad (not within the authorization of PD/NSC-9) or an electronic surveillance abroad (not within the authorization of NSCID-6 or PD/NSC-9), either an extraordinary judicial warrant or specific Presidential approval of the search or surveillance is required.

With respect to the exigent circumstances exception to the warrant requirement, this exception applies in circumstances where, but for the emergency situation, a warrant would be applied for and would issue. The exception would also apply if the President had delegated his authority to the Attorney General to authorize warrantless physical searches to gather foreign intelligence and counterintelligence and the

*/ Again, PD/NSC-9 is the one exception to this statement.

~~SECRET~~

~~SECRET~~

search were made in circumstances where prior Attorney General approval could not possibly be obtained but would have issued had it been possible to make the prior application. In such a case, under Attorney General procedures the agency would be required, after the fact, to report the search and a description of the exigent circumstances to the Attorney General.

However, until the President makes a delegation of authority to the Attorney General, there can be no exigent circumstances exception to Attorney General approval as that approval could not issue in any event. And as the President himself has directly authorized only one specific search without a warrant, there is no pattern of precedents from which we can draw the standards which he might apply for taking such extraordinary action. Consequently, it cannot be said that but for the exigent circumstances, the President would have personally authorized the particular search.

The only remaining ground, therefore, for a warrantless search in exigent circumstances is that a judicial warrant would have issued but for the emergency which made application for and issuance of a warrant impossible. While the Department of Justice is of the view that extraordinary warrants can issue for physical searches to gather foreign intelligence and counterintelligence, neither the FBI nor the CIA has ever applied for such a warrant and no such warrant has ever

- 9 -

~~SECRET~~

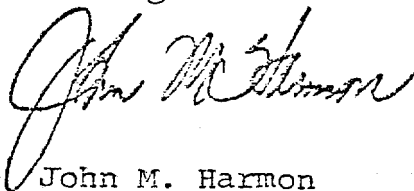
issued. Therefore, it cannot be said that but for the exigent circumstances a warrant would have issued because, based on past conduct, there would have been no application for a warrant even if there had been the opportunity.

The principle underlying the Fourth Amendment warrant requirement is that the standards for a finding of probable cause are to be set and applied by a neutral and detached magistrate. If warrantless physical searches are permitted in exigent circumstances even though warrants as a matter of policy would not be sought, there would never be judicial review of the standards being applied by the intelligence agencies to conduct such searches. Physical searches in foreign intelligence matters differ in this respect from warrantless searches in law enforcement in that the law enforcement search will often be subject to judicial review where the search is challenged in a subsequent criminal trial. However, the search for intelligence purposes will go unexamined and probably unknown. While this is true whether the search is pursuant to Presidential authorization or not, at least where the search is pursuant to Presidential authorization the standards have been articulated at the very highest level of the Executive Branch,

- 10 -

~~SECRET~~

and are not left to the discretion of lower officials. It is this point on which the court focused in United States v. Ehrlichman, ____ F.2d ____ (D.C. Cir. 1976), and it is this point which militates against even an exigent circumstances exception in the absence of a Presidential authorization. Consequently, in light of the practice of the intelligence agencies with respect to applications for judicial warrants and absent Presidential authorization, it is my view that there can be no warrantless physical searches or electronic surveillance abroad even in exigent circumstances.



John M. Harmon
Acting Assistant Attorney General
Office of Legal Counsel

June 1, 1977

PD/NSC-

TO: Attorney General
Secretary of State
Secretary of Defense
DCI

RE: Electronic Surveillance Abroad and Physical
Searches for Foreign Intelligence Purposes.

I have carefully reviewed the issues raised in the SCC's report with respect to warrantless electronic surveillance directed against United States persons abroad, and warrantless physical searches (a) of certain premises or property within the United States and (b) of the premises or property of United States persons abroad. These searches and surveillances would be conducted solely for foreign intelligence and counter-intelligence purposes, including intelligence on international terrorism.

I am informed by the Attorney General that in his view the President has the constitutional authority to approve warrantless electronic surveillance directed against Americans abroad who are agents of foreign powers, but that the Supreme Court has never addressed this issue.

He also informs me that in his view the President has the constitutional authority to approve reasonable warrantless physical searches directed against foreign

~~SECRET~~

~~SECRET~~

Sanitized Copy Approved for Release 2011/01/26 : CIA-RDP79M00095A000300010001-0

powers or their agents in the United States and against Americans abroad who are agents of a foreign power. He notes, however, that no court has ever recognized this authority, so that his opinion on this issue is subject to judicial challenge.

It is clear to me that reasonable physical searches and electronic surveillances for intelligence purposes necessary to the security and well-being of our nation should be authorized. The invocation of inherent Presidential powers to authorize such searches and surveillances, however, would subject such searches and surveillances to doubt and question not only by those who are concerned about the proper role of our intelligence agencies but also by those who must carry out the searches often at grave risk to themselves. Therefore, it is my firm belief that this Government's clandestine intelligence activities -- and especially those which impact on the rights of Americans -- should to the maximum extent possible be legitimized and affirmed by the Congress as the lawmaking body of this nation. Such affirmation is essential not only as reassurance to the Nation that our intelligence activities are conducted

- 2 -

~~SECRET~~

in a legal and proper manner but also as a national statement that these activities are necessary and desirable for the security and well-being of the American people. Therefore, I direct that the Department of Justice, in coordination with the Department of Defense, the Department of State, the Central Intelligence Agency, and the Vice President, produce draft legislation

with respect to electronic surveillance abroad and physical searches both in the United States and abroad to be presented to Congress by this Administration. It is my desire that these drafts be ready for my decision by July 31, 1977.

I am satisfied, however, that if compelling situations arise prior to such time as this legislation might be enacted, it may be necessary to the security and well-being of this Nation to engage in physical searches in the United States and physical searches and electronic surveillance abroad directed against United States persons.

- 3 -

~~SECRET~~

Therefore, pending the enactment of legislation in this area, I delegate the power to the Attorney General and his successors in office, to approve, without prior judicial warrant, electronic surveillance directed against United States persons abroad.

This power and authority shall be exercised pursuant to the following standards and procedures:

(1) A warrantless, non-consensual electronic surveillance abroad directed against a United States person will, except in emergency situations, only be authorized upon the personal approval of the Attorney General (or Acting Attorney General), upon the request of the head of the Department or Agency desiring the electronic surveillance.

(2) Approval will not be granted unless the Attorney General (or Acting Attorney General) has satisfied himself that:

(a) the requested electronic surveillance is necessary to obtain significant foreign intelligence or counterintelligence information;

(b) the United States person who is the target of the electronic surveillance is an agent of a foreign power; and

- 4 -

~~SECRET~~

(c) the minimum physical intrusion necessary to obtain the information sought will be used.

(3) Where necessary, the request and authorization may be oral, but shall be followed by written confirmation as soon as possible.

(4) No electronic surveillance directed against a United States person shall continue for over 90 days without the written authorization of the Attorney General (or Acting Attorney General).

(5) In addition, I authorize the Attorney General to adopt procedures governing the conduct of electronic surveillance abroad, whether or not directed against a United States person, to ensure its legality and propriety, which procedures shall provide for authorization in emergency situations and for the minimization of the acquisition, retention, and dissemination of information concerning United States persons which is not necessary for legitimate Government purposes.

* * *

I have already in my February 3, 1977, memorandum authorized and delegated the power to the Attorney General to approve the minimum necessary trespass or intrusion to

- 5 -

~~SECRET~~

implant an electronic surveillance device. I hereby delegate the power to the Attorney General to adopt procedures concerning, and to approve, certain warrantless physical searches of (a) the real or personal property of foreign powers in the United States, and (b) the personal property of persons in the United States or United States persons abroad who are agents of foreign powers. These physical searches shall be limited to (a) a search of personal property which is in the custody of the United States or its agents, or (b) a search of the premises of a foreign power by an agent of the United States who is lawfully on the premises, which extends beyond those specific areas to which the agent is entitled to have access.

This power and authority shall be exercised pursuant to the following standards or procedures:

(1) A physical search of the property or premises of a foreign power in the United States will only be authorized pursuant to procedures adopted by the Attorney General to insure its reasonableness, which procedures shall not authorize any breaking or non-consensual entering of any real property.

(2) (a) A physical search of the personal property of persons in the United States or a United States person

abroad will, except in emergency situations, only be authorized upon the personal approval of the Attorney General (or Acting Attorney General), upon the request of the head of the Bureau or Agency desiring the search.

(b) Approval to conduct such a search will not be granted unless the Attorney General (or Acting Attorney General) has determined that:

(i) the requested search is necessary to obtain significant foreign intelligence or counter-intelligence information;

(ii) the person whose property is to be searched is an agent of a foreign power;

(iii) the minimum physical intrusion necessary to obtain the information will be used; and

(iv) the search does not involve the breaking or non-consensual entering of any real property and any container to be searched is, at the time of the search, in the lawful custody of the United States or its agents.

(c) Where necessary, the request and authorization may be oral, but shall be followed by written confirmation as soon as possible.

- 7 -

~~SECRET~~

~~SECRET~~

(3) I am not delegating the authority to make any physical search within the United States or of the property of United States persons abroad for foreign intelligence or counterintelligence purposes that involves the breaking or non-consensual entering of any real property or the search of any personal property which is not in the custody of the United States or its agents, except in emergency situations where a person's life is reasonably believed to be in imminent danger.

(4) In addition, I authorize the Attorney General to adopt procedures governing the conduct of physical searches authorized herein to ensure their legality and propriety, which procedures shall provide for authorization in emergency situations and for the minimization of the acquisition, retention, and dissemination of information concerning United States persons which is not necessary for legitimate Government purposes.

* * *

Nothing in this directive shall be deemed to authorize the warrantless opening of mail in United States postal channels, nor shall anything in this directive be deemed to affect PD/NSC-9.

Jimmy Carter

- 8 -

~~SECRET~~

Wgc 77-3456
27 May 1977

MEMORANDUM FOR: PRM/NSC-11 Subcommittee Members

FROM : 25X1
General Counsel

SUBJECT : Lack of Authority for Electronic Surveillance Abroad
and Physical Searches Within and Without the United
States

REFERENCE : Draft Report to the Special Coordination Committee,
Same Subject, dated 13 May 1977, Prepared by
Department of Justice

1. The referenced report deals with warrantless physical searches of foreign powers or their agents in the United States, and warrantless searches or electronic surveillance directed against U.S. persons abroad and conducted for the purpose of gathering foreign intelligence or counterintelligence. Attached to the draft is a legal memorandum. That memorandum concludes that while the President has the constitutional power to approve the activities in question, he has never delegated that authority except within narrow limits (NSCID-6 and PD/NSC-9), and that absent such a delegation, or absent specific President's approval in a particular case, no such activities may lawfully be conducted by CIA, even under exigent circumstances in which a warrant might not otherwise be required if the search or surveillance was intended for some purpose other than the gathering of foreign intelligence.

2. Starting with the premises developed in the attached memorandum of law, the referenced report considers steps that might be taken to place approval of the activities in question on a sound and workable legal footing. As a permanent step, the report proposes legislation "which would require warrants for physical searches within the United States along the lines of the present electronic surveillance legislation, and either warrants or statutory authorization with civil liberties safeguards for electronic surveillance and physical searches abroad." The recommendation is that such legislation be drafted by the Subcommittee, to be ready for the President's review by 31 July 1977. As an interim step, pending the submission and enactment of legislation, the report outlines four options and recommends the first of those options - namely, a limited delegation from the President that would authorize the Attorney General to approve, within a defined range of circumstances, warrantless physical searches in the United States and abroad and electronic surveillance abroad.

25X1

CLASSIFIED BY
EXEMPT FROM GENERAL DECLASSIFICATION
SCHEDULE OF E. O. 11652, EXEMPTION CATEGORY:
§ 5B(1), (2), (3) or (4) (circle one or more)
AUTOMATICALLY DECLASSIFIED ON
<i>Indefinite to Determine</i>
(unless impossible, insert date or event)

~~SECRET~~

A draft delegation is also attached to the report, and among other things the delegation contains a proposed Presidential statement as to the need for legislation affirming the power of the Executive to conduct these activities and regulating the exercise of that power.

3. CIA's comments on the referenced draft report are set forth below.

The basic premise

4. It is likely to appear strange to the Special Coordination Committee that the issue of lack of authority in this field is being raised at this juncture, more than a year after the adoption of E.O. 11905 and the issuance of interim Attorney General procedures relating, in CIA's case, to electronic surveillance abroad, implementing Section 5(b)(2), and unconsented physical searches abroad, implementing Section 5(b)(3). Accordingly, by way of background, we think the report to the SCC should include an explanatory comment to the effect that the need for a further delegation of authority from the President has only recently been perceived. Whether on the theory that E.O. 11905 itself constituted a sufficient delegation, or that the Attorney General was in a position to act as the President's "alter ego" in regard to the authorization of activities covered by Sections 5(b)(2) and 5(b)(3), see U.S. v. Erlichman (D.C. Cir. No. 74-1882, decided 17 May 1976, slip op. page 31), Meyers v. U.S., 272 U.S. 52, 133 (1926), we believe it to have been the view of the last administration, including former Attorney General Levi, that no further action by the President was required to authorize the Attorney General to approve warrantless physical searches or electronic surveillance conducted by CIA abroad and directed against U.S. persons.

5. As we see it, no President could have signed an Executive Order providing that certain activities could be undertaken pursuant to procedures established by the Attorney General without understanding, and intending, that the Attorney General could thereafter approve such activities. We therefore doubt the need for a further delegation. But assuming such a need, the shift in Justice Department thinking on this point should be acknowledged.

The commitment to legislation

6. The draft report urges that legislation be submitted to the Congress which would recognize and affirm the search powers with which the report deals, and the attached draft delegation contains a Presidential commitment to this course of action.

7. In the case of searches outside the United States, the draft report and delegation are both careful to avoid any reference to a warrant requirement as an essential element of the proposed legislation. Nevertheless, it seems to

2
~~SECRET~~

us that the legislation inevitably will be shaped, either as submitted or as enacted, to include such a requirement. Depending on the showings that would have to be made in the application papers, and the detail of the information necessary to support such showings, a warrant requirement could as a practical matter rule out any CIA searches abroad, whether physical or electronic, directed against U.S. persons (who presumably would be the only ones protected). A commitment to legislation is therefore premature in our judgment. The better course would be a commitment to the consideration of a statutory approach, with a report examining the pros and cons rather than a draft bill scheduled to be presented to the President by the 31 July deadline.

Ad hoc warrant option

8. One of the possible interim options discussed in the draft report is to forego any delegation of authority from the President, leaving the Attorney General assertedly powerless to approve any warrantless searches abroad, or physical searches within the United States, and instead to seek special judicial warrants on a case-by-case basis. In terms of its availability as an alternative, this option is put forward as being on a par with the others, and the only issues deemed to require discussion in the report are policy issues.

9. Our impression is that there is considerable uncertainty surrounding the question of judicial authority to issue warrants for the purpose of gathering foreign intelligence. No such authority stems from either Rule 41 of the Federal Rules of Criminal Procedure or Title III of the Omnibus Crime Control and Safe Streets Act. Nor are there any other statutory provisions of which we are aware that even refer to foreign intelligence warrants, let alone authorize the issuance of such warrants or spell out the applicable procedures or describe the circumstances under which such warrants may be obtained.

10. If indeed there are important uncertainties in this regard, as we believe there are, the discussion of the special warrant option should be revised to indicate that the availability of this alternative is subject to legal question.

The scope of the delegation

11. The proposed delegation from the President, attached to the draft report, is limited in scope but would authorize the approval of warrantless searches, whether physical or electronic, in those circumstances in which CIA is likely to have an interest in carrying out such activities. Accordingly we have no objection to the limited scope of the delegation. However, we note

that the Attorney General's authority to approve warrantless searches directed against a U.S. person abroad is limited to situations in which the target is an "agent of a foreign power." We assume that the term "agent of a foreign power," which is not a defined term, includes, as it does under the definitions in the existing electronic surveillance procedures, one who is reasonably believed to be engaged in clandestine intelligence activities or sabotage at the direction of a foreign power, or one who knowingly aids or abets such a person in such activities. We also assume that term includes, again as it does under the definitions in the existing electronic surveillance procedures, a person who is reasonable believed to be engaged in terrorist activities or acting on behalf of a foreign terrorist group. We believe the draft delegation should be amended to clarify these points and to specify that the Attorney General's authority extends to the approval of a warrantless search or surveillance directed against a U.S. person abroad reasonably believed to be involved in terrorist-related activities.

25X1

1	Sanitized Copy Approved for Release 2011/01/26 : CIA-RDP79M00095A000300010001-0		
2			
3			
4			
	ACTION	DIRECT REPLY	PREPARE REPLY
	APPROVAL	DISPATCH	RECOMMENDATION
	COMMENT	FILE	RETURN
	DISCREPANCY	INFORMATION	SIGNATURE
REMARKS:			
FROM: NAME, ADDRESS, AND PHONE NO.			DATE

CONTROL NO. _____

Handle Via

COMINT

Channels

Access to this document will be restricted to
those approved for the following specific activities:

Warning Notice

Sensitive Intelligence Sources and Methods Involved

NATIONAL SECURITY INFORMATION

Unauthorized Disclosure Subject to Criminal Sanctions

~~Top Secret~~

(Security Classification)
E2 IMPDET

REPORT TO THE SCC -- ATTORNEY GENERAL PROCEDURES

EXECUTIVE SUMMARY

The attached report is submitted to the SCC pursuant to PRM/NSC-11 by the subcommittee acting under the direction of the Attorney General.

The report addresses problems identified with Attorney General procedures governing electronic surveillance (including SIGINT under Section 5(b)(2), E.O. 11905.

The subcommittee concludes that the Attorney General procedures do not seriously impair the government's ability to obtain that foreign intelligence and counterintelligence information which legally can be obtained by electronic surveillance.

Of the problems identified, several were determined to be insoluble because they arise from legal requirements, see Problem (a) (pages 4-5); Problem (e) (pages 16-18); Problem (f) (pages 19-19a); Problem (h) (pages 23-25).

Problem (b) (pages 6-9), relating to the requirement to delete the identities of U.S. persons from communications, even when they are not parties to the communication, except under specified conditions, is more a matter of policy than law, but the subcommittee recommends that current policy be maintained, except as modified below.

Problem (c) (pages 10-11) relates to the powers of

~~TOP SECRET UMBRA~~
HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

the Attorney General to go behind certifications by other Executive officials. A change to the Attorney General's powers would require a change in the President's delegation to the Attorney General, and the subcommittee recommends against such a change.

Problem (d) (pages 12-15) concerns the effect of the Attorney General's deletion requirement on data base maintenance and the administrative burden associated with reports to the Attorney General concerning cases where identities are not deleted. In addition, it discusses the deletion requirement where United States persons are parties to the intercepted communications. The subcommittee recommends that the procedures not be changed except as discussed below.

Problem (g) (pages 20-22) involves the impact of the Attorney General procedures on the reporting of economic information. Here the deletion requirements noted above have an adverse impact on reports concerning export/import cases, because of deletion of equipment nomenclature, and concerning certain commodity and fund movements, because masking the identity of the U.S. corporation can lead to double counting or a lack of effective targeting of collateral sources. The

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET UMBRA

Sanitized Copy Approved for Release 2011/01/26 : CIA-RDP79M00095A000300010001-0

subcommittee recommends that the Department of Justice and collectors/customers identify those areas where corporate identities are important to the understanding of significant foreign intelligence, and that the procedures be amended to allow reporting of corporate identities in those areas.

Problem (i) (pages 26-37) relates to the problem of the interface between law enforcement and foreign intelligence electronic surveillance. As noted above, the deletion requirements are more a matter of policy than law, and that is especially so in this area. Enforcement agencies are desirous of obtaining information from intelligence agencies' electronic surveillance, particularly in the areas of terrorism and international narcotics trafficking. Intelligence agencies are concerned about mixing law enforcement and foreign intelligence activities and in addition are concerned for the protection of their sources and methods. The problem in the narcotics field has also been studied by the Office of Drug Abuse Policy. The subcommittee is unable to make a final recommendation on this issue.

Problems (j) and (k), briefly mentioned in the report, were not pertinent to this report.

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET UMBRA

Sanitized Copy Approved for Release 2011/01/26 : CIA-RDP79M00095A000300010001-0

Finally, a problem with specific reference to the Attorney General's procedures relating to TELEX and leased line interceptions has been raised by NSA (pages 39-41). NSA recommends generally reducing the role of the Attorney General and the Department of State in favor of accepting intelligence agencies' determinations. The subcommittee recommends against this proposal.

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Sanitized Copy Approved for Release 2011/01/26 : CIA-RDP79M00095A000300010001-0

REPORT TO THE SPECIAL COORDINATION COMMITTEE

Re: Attorney General Procedures Relating
to Electronic Surveillance.

This report is submitted to the SCC by the SCC subcommittee acting under the direction of the Attorney General pursuant to PRM/NSC-11.

This report discusses the problem areas which have been identified in the year since Attorney General procedures have been in effect. Where those problems are legal in nature, the report reflects the Department of Justice's conclusion as to the limits of the law. Where the problems are not legal in nature, the report attempts to identify the competing considerations involved so that the SCC may make an informed policy recommendation.

Since March 1, 1976, pursuant to Section 5(b)(2), E.O. 11905, all electronic surveillance, including signals intelligence, which is directed against communications to or from the United States or against United States persons abroad is prohibited except lawful electronic surveillance conducted in accordance with procedures approved by the Attorney General.* / In fact, the procedures place

* / In addition, on April 8, 1977, pursuant to PD/NSC-9 the Attorney General adopted procedures to govern the conduct of electronic surveillance in Berlin.

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

restrictions on CIA and NSA which extend beyond electronic surveillance directed at communications to and from the United States or against United States persons abroad. Except for CIA's procedures for microphone surveillance, the Attorney General's procedures for NSA and CIA also place restrictions on the retention, use, and dissemination of all communications which either have a United States person as a party or which mention an identifiable United States person. Almost all of the procedures have been amended at least once in light of operating experiences and problems encountered in the original procedures.

In addition, all FBI electronic surveillance within the United States, while not subject to the provisions of Section 5, E.O. 11905, must be personally approved by the Attorney General and is subject to case-by-case restrictions on the retention and use of information, and most recently, general restrictions on dissemination.

The basic structure of the Attorney General's procedures with respect to CIA's and NSA's interception of electronic communications is: (1) to require the prior approval of the Attorney General before any United States person may

- 2 -

TOP SECRET UNBRA
HANDLE VIA COMINT CHANNELS ONLY

be targeted, which approval can be granted only if the United States person is an agent of a foreign power,*/ (2) to require the destruction of all intercepted communications which have a United States person as a party unless the communication contains significant foreign intelligence or other information specified in the procedures, and (3) to require the deletion of the identity of any United States person reflected in an intercepted communication, even if he was not a party to the communication, unless certain strict criteria are met. Generally, these restrictions are required because in the Department of Justice's view they are necessary to ensure the lawfulness of the activity absent a warrant.

These procedures and their impact on the legitimate activities of the intelligence community were the subject of an extensive review in the last Administration by a group under the direction of the DCI pursuant to a request from the NSC. While certain

*/ The definition of United States person in these procedures is quite broad, including any person for whom a warrant would be required if the electronic surveillance were for other than foreign intelligence purposes. Here too, the Attorney General's procedures extend further than the mandate of Section 5(b)(2), E.O. 11905. See pages 16-18, infra.

- 3 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

specific problems were identified in that review, the conclusion was that:

No problems were identified which would seriously impair our present ability to produce meaningful foreign signals intelligence on economic, political and military matters of significant importance to the maintenance of national security or the effective conduct of foreign policy, nor which would impair our present ability to predict foreign crises.

The following problem areas were identified in the DCI's report.

PROBLEM AREAS

Problem (a) --

The categorization of strictly foreign intelligence signals intercept operations under the general heading of "electronic surveillance." This has the effect of placing SIGINT operations under the same strictures and control procedures as are applied to other more extraordinary and classic electronic penetration or eavesdropping activities.

- 4 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

The Department of Justice is of the view that for legal purposes SIGINT operations are not distinguishable from "more extraordinary and classic electronic penetration or eavesdropping activities." That is, communications on ILC are protected under the Fourth Amendment in the same manner as communications on telephones. If a party to a communication is a person entitled to Fourth Amendment protections, those communications are protected by the Fourth Amendment and their interception must be consistent with Fourth Amendment requirements.

Whether foreign powers in the United States, or their officers and employees while acting in an official capacity, are protected by the Fourth Amendment at all is an open question. They are, however, protected by international law and treaty, but the Department of Justice and the Department of State agree that the interception of foreign powers' communications are not prohibited by international law or treaty. Under the various procedures, electronic surveillance of foreign powers is not affected except to the extent that United States persons may be involved as parties to or subjects of communications.

In short, the Department of Justice concludes that the placing of SIGINT operations under the same strictures and controls as are applied to other forms of electronic surveillance is legally necessary.

- 5 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

The Attorney General's guidelines for the conduct of SIGINT operations against international lines of communications and national diplomatic nets make no clear-cut distinction between information concerning "United States persons" derived from intercept of dedicated foreign National Diplomatic Communications on the one hand (or even from intercept of those communications of foreign affairs ministries which are passed via certain regularly used International Commercial links), as opposed to information obtained from intercept operations directed against the international communications of purely private individuals and entities.

The Attorney General's procedures require the deletion of the identity of United States persons from intercepted communications, except when certain specific exceptions are met,*/ whether or not the United States person is a party to the communication. Under current judicial case law a

*/ The exceptions are: the communication is enciphered or reasonably believed to contain secret information; the retention of the communication is necessary for the maintenance of technical data bases; the communication evidences or concerns a possible threat to the physical safety of any person; the communication is evidence that the U.S. person may be an agent of a foreign power; the communication is evidence that the U.S. person may be a target of intelligence activities of a foreign power; the communication is evidence that the U.S. person is engaged in the unauthorized disclosure of properly classified national security information; the U.S. person has consented to the retention and use of communications to which he is a party or in which he is mentioned; the communications have been intercepted pursuant to prior Attorney General authorization of the selection term; the communication contains information relating to the safety of any Secret Service protectee; or the identity of the U.S. person in the context of the message is significant foreign intelligence.

- 6 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

person does not have a protected Fourth Amendment interest in what others communicate about him, and it has therefore been suggested that this requirement of deletion is unnecessary when the United States person is not a party. As a strictly legal matter deletion in most cases may not be required.*/
As a policy matter, however, Attorney General Levi determined that such deletions were desirable where one of the specific exceptions did not apply. In addition, it was felt that previous political abuse of information concerning United States persons acquired from communications to which they were not parties would, if the matter came before a court, threaten SIGINT operations generally and perhaps result in a judicial decision finding a Fourth Amendment interest in what others communicate about a person.

Prior to the Attorney General's procedures, pursuant to Henry Kissinger's instructions all intercepted communications making reference to him were passed to him for review. He then decided whether and to whom they should be disseminated. This system, for the most part, was used for legitimate purposes, but in other cases for political advantage and personal gossip. It was to limit use of information concerning United States persons to legitimate purposes that the restrictions were adopted on the dissemination of

*/ Deletion, where there is no legitimate governmental need for the information, would be required by the Privacy Act. See 5 U.S.C. §552a(e)(1).

the identity of United States persons whether or not they were parties to the intercepted communications. During the 1976 election campaign, for instance, a number of foreign power communications were intercepted regarding confidential statements made by candidate Carter to his advisers or by his advisers. With rare exception these communications were not disseminated or used.*/ Dissemination or use was allowed only where necessary to assess the knowledge and intentions of the foreign powers themselves in terms of what activities or lack thereof might be motivated by their information on candidate Carter.

NSA points out, however, that names are often the single means of relating otherwise seemingly unrelated events, and their deletion can frustrate the completion of a comprehensive intelligence report. In addition, deletion of the identifying context often results in the deletion of information which may be pertinent to an intelligence analyst.

The Department of Justice recognizes that the list of exceptions under which the identity of a United States person can be revealed perhaps could be expanded to allow dissemination in other areas while still maintaining the protection against

*/ The Attorney General's procedures require not only the deletion of a name, but any other information which would identify the United States person. In the case of these communications virtually the entire communication had to be deleted so as not to identify candidate Carter.

- 8 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

misuse of political and personal information. See Problems (g) and (i), infra. However, any expansion of the present list of exceptions should be undertaken only after a careful balance of the actual need for the identity of the United States person against the potential for abuse of such information.

Options:

(1) Amend the procedures to eliminate the deletion requirement where a United States person is not a party to the communication to permit the retention of information identifying U.S. persons, except where personal or domestic political information is involved.

(2) Except as recommended with respect to Problems (g) (corporate identities) and (i) (law enforcement purposes), leave the current deletion requirement intact.

Recommendation: The subcommittee recommends Option (2).

- 9 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Problem (c) --

In certain instances, such as in the determination of what SIGINT computer selection terms pertaining to United States persons may or may not be used, the current guidelines vest in the Attorney General the responsibility for personally determining in each case if the information being sought constitutes significant foreign intelligence and that such information cannot be obtained by means other than "electronic surveillance."

Under the Attorney General's procedures relating to NSA and CIA before a United States person can be targeted the Attorney General must satisfy himself among other things that significant foreign intelligence information is sought and that the information cannot be obtained by less intrusive means. Where such matters are certified to by high Executive officials with expertise in the relevant areas, the Attorney General, of course, gives great weight to the certification. However, the President's memorandum to the Attorney General delegating him the authority to approve electronic surveillances within the United States explicitly places in the Attorney General the final responsibility to determine whether the particular electronic surveillance is "necessary." For electronic surveillance outside the United States, there is no such explicit memorandum, but the Department of Justice

- 10 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

believes that a similar responsibility -- to the extent the Attorney General has any authority to approve such surveillances -- must be inferred. Therefore, until such time as legislation creates an independent magistrate and legitimizes such activities on another basis, the Department of Justice is of the opinion that where the President has delegated to the Attorney General the President's powers with respect to warrantless surveillances of United States persons, the President's power clearly includes the final determination as to the necessity of the surveillance, which requires a decision as to the significance of the foreign intelligence sought and the feasibility of using less intrusive means to acquire the information.

Options:

(1) Have the President place the responsibility for determining the significance of the information sought and the feasibility of using less intrusive means in a person other than the Attorney General.

(2) Leave the Attorney General's current powers unchanged.

Recommendation: The subcommittee recommends Option (2).

- 11 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Problem (d) --

The detailed Attorney General guidelines for SIGINT ILC/NDC operations contain particularly strict rules against revelation of the identities of "United States persons" noted in foreign communications and against the maintaining of computer selection terms using such names. This impedes reporting and data base maintenance, and creates administrative accountability burdens for SIGINT collectors.

As noted above, under Problem (b), the restriction on reporting the identities of United States persons who are not parties to intercepted communications is based largely on policy rather than legal considerations. When the United States person is a party, legal considerations also come into play. Inasmuch as the President's power to proceed without a judicial warrant is limited to the gathering of foreign intelligence, it cannot be used to gather domestic intelligence merely by targeting non-United States persons and providing the intelligence collectors with a "watch list" of Americans whose contacts with the non-United States target were to be reported. The Department of Justice, of course, recognizes that to

- 12 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

understand the activities of foreign powers may require knowledge of the United States persons with whom the foreign powers deal. And again the Department of Justice believes that the list of specific exceptions to the deletion requirement perhaps could be expanded in light of identified areas where the identity of United States persons is necessary to the comprehension of information concerning foreign powers. As the procedures currently exist, there is one general exception to the deletion requirement where the identity of the United States person in the context of the communication is itself significant foreign intelligence information.

It may be more desirable to identify the additional particular areas where the identity is likely to be important to an understanding of the information concerning a foreign power, rather than rely on a broad construction of the general exception.

As to the impeding of data base maintenance, there is a specific provision excepting from the deletion requirement situations where the identity is necessary to the maintenance of technical data bases. Thus, it is not

- 13 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

HANDLE VIA COMINT CHANNELS ONLY

believed that the maintenance of the collector's data base is impeded, but it may be true that intelligence data bases generally may be impeded to some extent, see Problem (g).

Finally, the Department of Justice has not seen or heard evidence of any significant administrative burden involved in the requirement to report to the Attorney General annually the number of and basis for disseminations which include the identity of United States persons. NSA represented to the Justice Department that this requirement could be easily handled by computer. With respect to CIA, after an initial problem in setting up the operation in light of the procedures, the Department of Justice was led to believe that the reporting requirement would not be a serious burden. NSA states that an administrative burden has been discovered relating to the need to recall and reissue reports where it has been determined after the fact that a person was indeed a United States person. This occurred on 48 occasions in the last 10 months of 1976. The Department of Justice does not believe that this history justifies at this time a change in the procedures. Moreover, NSA's use of a title rather than a name to report identities

- 14 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

of Government employees does not alter the fact that their identities are being reported. Where identities are reported, an annual report to the Attorney General is the minimum that can be required to provide an opportunity to oversee NSA's performance under the procedures and the effect of the procedures. An alternative which has not been fully explored would be obtaining the consent of persons with COMINT clearances (or those persons with COMINT clearances who are likely to be parties incidentally intercepted or mentioned in intercepted communications). While the current procedures require reports even as to dissemination of identities pursuant to consent, the Department of Justice would be willing to lift this reporting requirement, because it would not constitute an unconsented use of information.

Options:

(1) Amend the procedures, in coordination with collectors and customers, to make a limited expansion of the current list of exceptions to permit the retention and use of incidentally intercepted communications to which a United States person is a party.* /

* / See Problems (g) and (i), *infra*.

- 14a -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

HANDLE VIA COMINT CHANNELS ONLY

(2) Except as recommended with respect to Problem (g) (corporate identities) and (i) (law enforcement purposes), leave the current deletion requirements intact.

(3) Obtain, or seek to obtain, the consent of persons with COMINT clearances to use and disseminate communications to which they are parties or which mention them without deletion of their identities.

Recommendation: The subcommittee recommends Option (2).

- 15 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Problem (e) --

The Attorney General's expanded definition of "United States persons," to include "any other alien known to be presently in the United States," greatly enlarges the scope of "electronic surveillance" restrictions and impacts in several areas; not the least of these is the basic problem of how to determine who is or is not an alien person or entity for the purposes of foreign intelligence.

The Attorney General's procedures define United States persons in a fashion much broader than E.O. 11905. In addition to United States citizens and permanent resident aliens, who are United States persons under the Order, all aliens lawfully or unlawfully in the United States are deemed United States persons unless they are officers or employees of foreign powers. While it galls many that an illegal alien in the United States should be entitled to full Fourth Amendment protections, court cases at the present time mandate such a conclusion. Indeed, in the Abel case the Supreme Court involved itself in an extended analysis to determine whether Colonel Abel's Fourth Amendment rights were violated, notwithstanding the fact that he was an illegal alien who was a high officer in a Soviet intelligence service.

- 16 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Others have questioned the need for Fourth Amendment protections where no criminal prosecution will be involved. The Fourth Amendment, however, is not primarily a protection from using evidence in a criminal prosecution -- although the suppression of evidence obtained in violation of the Fourth Amendment is a means by which the Amendment is enforced. It is, as its language indicates, a protection against unreasonable searches and seizures by the Government no matter what the purpose of the search or seizure. Its essence is to protect a person's justifiable expectation of privacy from Government invasion. Thus, its protections extend equally to searches for intelligence purposes as well as for law enforcement purposes. See United States v. United States District Court, 407 U.S. 297 (1972); Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975).

In fact, by excluding non-U.S. citizens and permanent resident aliens who are officers and employees of a foreign power from the definition of a United States person, the Department of Justice is giving to the intelligence community the benefit of the doubt as to the Fourth Amendment protections afforded such persons to the extent they act in their official capacity.

E.O. 11905 also includes within its definition of United States persons "corporations or other organizations incorporated or organized in the United States." As to organizations, the Order's definition is underinclusive in describing organizations subject to Fourth Amendment protections, see Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144 (D.D. C. 1976), so the definition in the Attorney General's procedures was appropriately expanded. With respect to corporations, the Order's definition was felt to be overinclusive because corporations incorporated in the United States which in effect act as extensions of foreign governments, again giving to the intelligence agencies the benefit of the doubt as to the Fourth Amendment's protection of foreign governments in the United States, were not thought to be entitled to the full protections of the Fourth Amendment. Finally, the pure incorporation test, while simple in application, was thought to provide a means by which foreign corporations could avail themselves of artificial protection merely by incorporating in the United States. Thus, a principal place of business test was used instead.*/

While the effect of the definition of United States person in the procedures is at times difficult of application, the Department of Justice believes it is legally required.

*/ The Department of Justice has no particular need to maintain the principal place of business test, and if its application is too difficult in practice, the simple incorporation test could be used in its place.

Problem (f) --

The current guidelines permit the identification in SIGINT reports of U.S. Government officials by name. NSA, however, has opted to restrict such reporting to the identification of such officials only by title. This was done because of the concern that the use of names will cause serious problems stemming from the provisions of the Privacy Act and the Freedom of Information Act.

This Problem is not in fact a problem with the Attorney General's procedures, but rather relates to NSA's voluntary practice. The Department of Justice and OMB, however, are of the opinion that reporting identities of persons by title rather than by name, where that title by itself or in the context of the communication is sufficient to identify the specific individual, does not take the material out of the definition of "system of records" in the Privacy Act, see 5 U.S.C. § 552(a)(5). That is, to the extent that a name is replaced by a title, but that title in the context of the message or by itself is sufficient to identify the specific person, NSA might as well report the specific name. This is not to say that the material, reported either by name or title, is a "system of records." To fit the statutory definition it must be a system "from

- 19

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."

Id. Thus, NSA may avoid the requirements to publish this material as a "system of records," see 5 U.S.C. § 552a(e)(4), by not retrieving the information by the person's name or title. If NSA is now retrieving by title, then it is OMB's and Justice's opinion that NSA must publish notice of a system of records.*/ If it is not now retrieving this information by title, then NSA can publish the names rather than titles and not be required to publish a notice if the material is not retrieved by name.

Reporting by name or title would not appear to have any relevance to the Freedom of Information Act.

*/ This notice can be as abbreviated for NSA as for CIA, compare 5 U.S.C. § 552a(j) with 552a(k).

- 19a -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Problem (g) --

There are prohibitions in the current guidelines against revelation in SIGINT reports of the specific identity of U.S. corporate entities. This sometimes impairs the usefulness of economic SIGINT reporting and precludes the identification of U.S. financial institutions handling OPEC funds, thus impeding the ability of the Intelligence Community to monitor petrodollar flow.

The requirement, discussed above with respect to Problems (b) and (d), that the identities of United States persons be deleted applies to corporate persons as well as natural persons. No specific exception with respect to corporations was requested by NSA because at the time it was believed that so long as NSA could retain the identity in its technical data base no identification in reports would be necessary. Generally this perception has proved true in application. Thus, NSA advised its consumers that there would be no significant effect on the quality or quantity of NSA production on bilateral and multilateral trade negotiations, international energy policy, international finance, political intelligence, nuclear proliferation, and military assistance intelligence.

- 20 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

The DCI's review for the NSC concluded that the procedures would not seriously affect the production and general analysis of reporting on major political, economic, and military subjects.

Nevertheless two specific problems have been identified in the deletion of corporate identities. First, in export/import trade cases, manufacturers' names or equipment nomenclature have been deleted, and this can negative any assessment as to the extent of high technology trade. Second, the masking of the identities of United States corporations hampers the correlation of information on the same subject obtained from collateral sources (e.g., it can result in the double counting of OPEC fund transfers) and impedes the effective targeting of intelligence requirements for collateral sources.

The Department of Justice recognizes the seriousness of both these problems and believes that the procedures can be amended in a manner to alleviate both problems consistent with law and the protection of justifiable expectations of privacy.

- 21 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

HANDLE VIA COMINT CHANNELS ONLY

Recommendation: The subcommittee recommends that the Department of Justice and collectors/customers identify those areas where corporate identities are important to understanding significant foreign intelligence, and that the Attorney General's procedures be amended in those areas so as not to require deletion.

- 22 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Problem (h) --

There are restrictions on the authority of SIGINT producers to collect and provide to the Secret Service certain SIGINT information relative to United States persons who are reasonably believed to constitute a potential threat to protectees.

At the present time the Attorney General's procedures allow NSA and CIA to disseminate any information incidentally acquired to Secret Service which information could otherwise be disseminated pursuant to E.O. 11905. Because of restrictions in the Executive Order itself, however, certain incidentally acquired information concerning the domestic activities of United States persons cannot be disseminated to the Secret Service. If the subcommittee's recommendation in its report on E.O. 11905 is adopted, Secret Service's problems with respect to incidentally acquired information will be cured.

The Secret Service, however, also desires the Attorney General's procedures to allow for the warrantless targeting of United States persons who the Secret Service believes pose

- 23 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

a threat to its protectees. To the extent that such United States persons are agents of a foreign power, as defined in the procedures, the procedures already provide for the possible warrantless targeting of such persons; but to the extent that such persons are not agents of a foreign power the Department of Justice is firmly convinced that such warrantless targeting would be unconstitutional.

The Department of the Treasury has submitted a memorandum to the Department of Justice providing national security and legal reasons why it considers the Attorney General's procedures should be modified to authorize NSA to use selection terms to target and intercept communications of United States persons where, based upon the facts presented to the Attorney General, there is reasonable cause to believe that the United States person may be a threat to the President, Vice President, or a visiting Head of State. Nonetheless, the memorandum cites no authority for the proposition that the Secret Service under its responsibilities to

- 24 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

protect the President, Vice President, Secretary of the Treasury, or foreign heads of state in this country are entitled to engage in warrantless searches of persons not suspected of being agents of foreign powers.*/*

*/ One case cited by Treasury, Scherer v. Brennan, 379 F.2d 609 (7th Cir. 1967) affirmed the dismissal of a civil suit against Secret Service agents on the grounds of official immunity; it did not reach the question whether a warrantless search by them would be constitutional. Indeed, in that case, the District Court made a finding of fact that the Secret Service agents had not made any search nor deprived the subject of any privacy.

- 24a -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

To the contrary, where there is probable cause that a person is about to commit a Presidential assassination, Congress has specifically provided for a court order to authorize the interception of wire or oral communications, see 18 U.S.C. § 2516(1)(c). Moreover, in Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975), the court held that unless a person was an agent of or collaborator with a foreign power, a prior judicial warrant was required before electronic surveillance could be conducted against the person, even though the surveillance was for protective purposes. And in United States v. United States District Court, 407 U.S. 297 (1972), the Supreme Court made clear that a domestic threat to the national security, no matter how grave, did not justify an exception to the warrant requirement. Given these court cases and the warrant requirement in 18 U.S.C. § 2516(1)(c), the Department of Justice remains of the firm view that warrantless electronic surveillance of a United States person for Secret Service protective purposes, unless the person is an agent of a foreign power, is constitutionally prohibited.

- 25 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Problem (i) --

There is, in the Executive Order and the Attorney General's guidelines, a sense of prohibition against cooperation between foreign intelligence agencies and law enforcement agencies which precludes fully effective foreign intelligence support to law enforcement activities. This is especially true in the narcotics area (which itself tends to fall outside the scope of defined "foreign intelligence") and affects most directly SIGINT support to DEA, Treasury/ Customs and the Coast Guard.

This problem area involves intelligence agency support to law enforcement agencies. Such support can take two forms -- active collection efforts on behalf of such agencies and reporting of information acquired in the course of foreign intelligence collection. The Executive Order clearly evidences a presumption against intelligence agencies participating in law enforcement activities. See Section 5(e)(1). It is the opinion of the Department of Justice, however, that while active collection efforts on behalf of law enforcement agencies is "participation" of the type prohibited to intelligence agencies, the mere reporting of information acquired in the course of foreign intelligence collection is not such "participation." Section 5(c)(1)'s statement that nothing in Section 5 shall prohibit dissemination to law enforcement agencies of incidentally acquired information indicating involvement in activities which may be in violation of law reinforces this conclusion. And the subcommittee's recommended amendment to Section 5(e)(2) would make this interpretation explicit in the Order. Finally, there is no constitutional

or statutory bar to information concerning crimes being disseminated to law enforcement agencies by intelligence agency collectors.

Although intelligence agency collection on behalf of law enforcement agencies is within the prohibited "participation" in E.O. 11905, there are certain exceptions. First, such participation is only prohibited within the United States. Second, in the areas of clandestine intelligence activity, international narcotics trafficking, and international terrorism participation is allowed even within the United States. And third, intelligence agencies may provide "specialized equipment or technical knowledge for use" by Federal law enforcement agencies. See Section 5(e)(1)&(2).

Finally, not all SIGINT collectors are always "foreign intelligence agencies" within the meaning of Section 5 of E.O. 11905. While NSA and CIA are for all purposes considered to be foreign intelligence agencies, which are barred from "participation" in law enforcement activities (except as described above), the military services' cryptologic agencies are a foreign intelligence agency only "while it is engaged in the collection of foreign intelligence or counterintelligence." On this basis, the Office of Legal Counsel, by letter of April 30, 1976, approved the Naval Security Group's active collection

- 27 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

efforts on behalf of the Coast Guard for its law enforcement needs.* /

The above discussion outlines the legal parameters (not including the Attorney General's procedures) within which intelligence agencies may support law enforcement agencies and activities. Specifically, under the Constitution, statutes and Executive Order, intelligence agencies may target electronic surveillance against spies, international terrorists, and international narcotics traffickers to support law enforcement agencies.**/ In addition they may disseminate to law enforcement agencies any information concerning violations of Federal law acquired in the course of foreign intelligence collection.

*/ An additional prohibition of Section 5(e)(1) of E.O. 11905 is that foreign intelligence agencies not fund law enforcement activities, and inasmuch as NSA provided all the funds for the Naval Security Group's operation, the Coast Guard was required to reimburse the Naval Security Group for the collection effort on behalf of the Coast Guard. In this way NSA funding of the collection effort was avoided.

**/ Intelligence agencies cannot target such persons without a warrant if they are United States persons, unless the United States person is the agent of a foreign power.

- 28 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

The Attorney General's procedures, however, create restrictions which are not otherwise required. Communications which have a United States person as a party must be destroyed unless they fall within certain exceptions. There is no general exception for information concerning crimes and there is no specific exception for information concerning narcotics trafficking, international terrorism, or clandestine intelligence activity, although there is a general exception for significant foreign intelligence information and there are specific exceptions for information concerning possible threats to the physical safety of any person, indicating a person is a target of a foreign intelligence agency, indicating the disclosure of classified information, or indicating that a person may be an agent of a foreign power. In addition, even where a United States person is not a party to a communication his identity must be deleted unless one of the above exceptions is met. The Department of Justice has informed NSA and CIA that "significant foreign intelligence information" would in almost all cases not include information concerning international narcotics trafficking.

- 29 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Thus, in practice under the Attorney General's procedures, a communication with a United States person as a party cannot be disseminated on the basis that it contains information concerning international narcotics trafficking, and it is instead destroyed in accordance with the procedures. And a United States person's identity cannot be revealed in any communication to which he is not a party solely on the basis that he is involved in international narcotics trafficking. In the terrorist area, the same is true with respect to United States persons who are terrorists, unless they act as agents of a foreign power (which includes a foreign-based terrorist group) or the communication itself evidences a possible physical threat to any person.* /

While there may be a certain negative impact from the procedures on the dissemination of information acquired by SIGINT regarding international terrorism and narcotics

* / The communications of domestic-based terrorists are, therefore, protected unless the communication is evidence of a threat to a person's physical safety.

- 30 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

trafficking, the real impact of the procedures appears to be on CIA wiretaps. And it is clear that in a number of instances important information regarding the identities and modus operandi of international narcotics traffickers has been lost due to the procedures.

In December, 1976, Attorney General Levi by letter to the Director, NSA, stated there was no legal requirement for these restrictions (other than the restriction on targeting United States persons). He noted that while DEA and Treasury/Customs were greatly desirous that these restrictions be lifted, NSA and CIA had objected to lifting the restrictions, for fear that it would result in a compromise of their intelligence sources and methods. Given this dispute, Attorney General Levi did not believe it was proper for him to change the existing procedures in this regard.*/ It is appropriate for the SCC to resolve this dispute.

*/ This discussion was included in a letter that authorized NSA to disseminate to DEA strategic narcotics intelligence, which had been a specific recommendation of the DCI's review.

- 31 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

DEA and Treasury/Customs continue to request that all information concerning international narcotics trafficking which can legally be disseminated to them in fact be disseminated to them.*/In addition, DEA requests that certain ILC channels be targeted by NSA to gather intelligence on international narcotics trafficking (this would not involve targeting any United States persons).

CIA and NSA, however, are concerned about the security of their sources and methods. With respect to SIGINT, disclosure would result in a loss of narcotics intelligence information as well as possible compromise of certain NSA techniques. With respect to CIA wiretaps, disclosure

*/ The Treasury Department notes that Customs authorization to search at border points is very broad, and that it is extremely remote that the "source" leading to an arrest would be subjected to a discovery motion, particularly in routine border searches. Even in a strip search or body cavity search, the "source" would be protected if the basis for the search were discovered during the border search. Thus, a routine border search is first accomplished and a strip or cavity search only conducted if Customs officers discover other articulable factors. In the rare case where a discovery motion is made and would possibly jeopardize a sensitive source, Customs would recommend that Justice forego prosecution to protect the source. (The contraband would at least have been removed from circulation.)

TOP SECRET UMBRA

Sanitized Copy Approved for Release 2011/01/26 : CIA-RDP79M00095A000300010001-0

could reveal CIA's unilateral electronic surveillance operations in a foreign country, thereby damaging CIA's liaison relationship there.

CIA has suggested its willingness to disseminate narcotics information concerning United States persons to DEA and Customs, provided that the information not be used for "law enforcement purposes." CIA believes in such a situation the identity of the United States person will not have to be indexed/ retained for purposes of responding

- 32a -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Sanitized Copy Approved for Release 2011/01/26 : CIA-RDP79M00095A000300010001-0

to 18 U.S.C. § 3504.* / CIA's belief here, however, is mistaken. Section 3504 motions, are made to discover whether or not an electronic surveillance was ever made of the particular person. The Department of Justice has taken the position in the past that where the intercepted communication is not used, retained, or disseminated -- or the identity of the intercepted party is deleted -- no record need be kept, so that an agency can make a negative response to a § 3504 motion. Whenever the communication is used, retained, or disseminated, however, without the identity of the United States person party deleted, the communication must be retained/indexed, no matter what the purpose of the use, retention, or dissemination.

The Department of Justice is currently reassessing its § 3504 guidelines, and it is likely that in the future

* / 18 U.S.C. § 3504 provides a motion whereby any party to any Federal proceeding may discover whether he has been subjected to electronic surveillance, and if so, whether the surveillance was lawful. While such motions are handled ex parte and in camera by the court, and while the Department of Justice is not aware of a single instance in which an intelligence surveillance has been compromised against an intelligence agency's wishes pursuant to such a motion, CIA and NSA feel very strongly that their surveillances should be protected from ever having to go to a court, even ex parte and in camera.

- 33 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

HANDLE VIA COMINT CHANNELS ONLY

whenever a United States person's communication is used, retained for use, or disseminated -- whether or not his identity is deleted -- his identity will have to be retained/indexed for § 3504 purposes.

Therefore, no matter for what purpose the information is retained or disseminated, CIA could not avoid the § 3504 indexing requirement. With respect to communications to which United States persons are not parties, however, the elimination of the requirement to delete the identities of United States persons mentioned would pose virtually no security risk to sensitive sources and methods, because under § 3504 only parties to communications have a right to make the motion. Therefore, where United States persons are merely mentioned, they could not discover that such information was obtained or used.

The following is the view of the Department of Justice concerning the possible risk to sensitive sources and methods that would be posed by dissemination of communications to which United States persons are parties.

- 34 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

whenever a United States person's communication is used, retained for use, or disseminated -- whether or not his identity is deleted -- his identity will have to be retained/indexed for § 3504 purposes.

Therefore, no matter for what purpose the information is retained or disseminated, CIA could not avoid the § 3504 indexing requirement. With respect to communications to which United States persons are not parties, however, the elimination of the requirement to delete the identities of United States persons mentioned would pose virtually no security risk to sensitive sources and methods, because under § 3504 only parties to communications have a right to make the motion. Therefore, where United States persons are merely mentioned, they could not discover that such information was obtained or used.

The following is the view of the Department of Justice concerning the possible risk to sensitive sources and methods that would be posed by dissemination of communications to which United States persons are parties.

- 34 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Were CIA to retain, use, or disseminate information from a United States person's communication relating to narcotics trafficking, and that person were to make a § 3504 motion in a criminal prosecution against him, CIA would have to submit to the court the facts surrounding the surveillance. These facts would be reviewed in camera and ex parte by the court; that is, the facts would be kept secret and not revealed to the person making the motion or to the public.*/ If the court determines that the over-hearing was lawful, no facts concerning the surveillance are disclosed to the person making the motion, although he is informed that at some time in some place he has been overheard and that the overhearing was lawful. If in the unlikely event the court were to determine that the surveillance was unlawful, the Department of Justice would either appeal the decision or dismiss the prosecution. In either case no disclosure would be made. The Department of Justice is not aware of any case where a civil suit has

*/ The Department of Justice reiterates that there has been no instance of any leak from a court pursuant to a § 3504 motion.

- 35 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

been instituted after a dismissal of prosecution following an ex parte determination of illegality. If it were to occur the Department would seek a protective order to prevent discovery, and if that were not successful, it could even stipulate liability so as to avoid disclosure. In short, the Department of Justice believes that the arguments based on experiences in civil cases having no relation to § 3504 motions concerning the threat to sensitive sources and methods posed by § 3504 are somewhat exaggerated. And it must be recognized by CIA that § 3504 is not avoided by not disseminating information to law enforcement agencies, because the mere use, retention, or dissemination for any purpose of United States person's communication is sufficient to require a response to a § 3504 motion.

Options:

(1) Amending the Attorney General procedures to exempt from the deletion requirements the identities of United States persons who are not parties to communications (a) whenever there is evidence they may be involved in any criminal activity, or (b) whenever there is evidence they may be involved in certain specified activities, e.g., clandestine intelligence activities, terrorism, or narcotics trafficking.

- 36 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

(2) Amending the Attorney General procedures to exempt from the destruction and deletion requirements the communications of United States persons incidentally intercepted (a) whenever there is evidence they may be involved in any criminal activity, or (b) whenever there is evidence they may be involved in certain specified activities, e.g., clandestine intelligence activities, terrorism, or narcotics trafficking.

(3) Not amending the Attorney General's procedures.
Recommendation: DEA and Customs/Treasury recommend Options (1)(b) and (2)(b). NSA recommends Option (3). CIA recommends Option 1(b) and does not object to Option 2(b), if the Department of Justice will agree to drop any prosecution when in CIA's view the prosecution will threaten CIA sources and methods.

Problem (j) --

Current U.S. laws and court actions, essentially the Privacy and Freedom of Information Acts and motions for disclosure claiming "electronic surveillance," tend to threaten the revelation of sensitive SIGINT sources and methods. This is caused by the absence of any general exemption for signals intelligence information and strict enjoinder against its use for evidentiary or prosecutive purposes in U.S. civil or criminal cases.

This problem is not in fact a problem with the Attorney General's procedures, but rather relates to statutory problems which are the subject of another report by this subcommittee.

- 38 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

Problem (k) --

There is no formal guidance relative to the conduct of "live" signals intercept training within the United States, similar to the existing procedures for the conduct of SIGINT Test and Evaluation activities.

This problem has never been formally raised with the Justice Department and it recommends that the applicable agencies present their views so that the Attorney General may offer the requested guidance.

In addition to the problems identified in the DCI's report, the subcommittee surfaced certain other concerns.

(1) Problems with the review and approval procedure for NSA requested, FBI conducted special wiretaps.

NSA believes that this review and approval procedure adversely affects NSA's ability to provide intelligence to aid the effective conduct of foreign policy. This is due, in NSA's view, to the possibility of interruption in coverage (which interruptions have occurred in the past)

- 39 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

and the number of people exposed to large amounts of information with consequent risks of disclosure.

NSA consequently recommends that the review and approval procedures for these wiretaps should be changed:

(1) to limit the Attorney General's approval to a determination of whether the target is a foreign power or an agent of a foreign power, and not allow him to assess whether useful intelligence information is sought or likely to be obtained;

(2) to limit the Department of State's role to assessing the political risk of the surveillance, and not allow it to assess the validity of the intelligence requirements;

(3) to allow the FBI "wide latitude to conduct feasibility studies and to develop operations plans and concepts upon the request of NSA;"

(4) to not require the review and approval process to expose "detailed information regarding cryptologic success"; and

(5) to greatly reduce the documentation required for 90 day renewals.

- 40 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

In the view of the Department of Justice, recommendations (1), (2), and (4) would require amendment of the President's memorandum to the Attorney General delegating to him the authority to approve electronic surveillances in the United States. With respect to recommendation (1), the Department of Justice opposes it for the reasons elicited in the discussion of problem (a) of the DCI's report. As to recommendations (2) and (4), the Department of Justice and the Department of State do not believe that the political risk can be assessed except in terms of the potential benefit to be gained by the surveillance (which may depend on cryptologic success) and the validity of the intelligence requirements. As to the FBI's latitude to conduct feasibility studies or to develop plans, the Department of Justice is not aware of any restriction on the FBI which interferes with the efficient conduct of studies or development of plans.

- 41 -

TOP SECRET UMBRA
HANDLE VIA COMINT CHANNELS ONLY

LOG NO: 1988

~~ER~~ FE

JOANNE MR

MK

Destroy


CY TO: _____

SENT : _____

FILE : _____

NNTC

NOTES:
25X1

For 
PRM-11 History
This, brother, is
Task 1 !

IC REGISTRY ROUTING SLIP

Rtg	Office	INIT	Date
	D/DCI/IC		
	EA		
1A	AD/DCI/IC		
1	EO	RK	8V6
2	SA [redacted]	25X1	
3	SA [redacted]		
	CFI (Sec't)		
	NFIB (Sec't)		
	Ch. Spt. Staff		
	Ch. Registry		
	CH, OPP		
	P&PD		
	IHD		
	SECOM		
	CH, OPBD		
	DSG		
	P&BDD		
	PAD		
4	CH, OPEI		
	Integ Staff		
	SIGINT Div.		
	IMAGERY Div.		
	HRD		
	PA&ID		



25X1

When circled - cy has been furnished.

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM:

General Counsel

EXTENSION

NO.

DATE

TO: (Officer designation, room number, and building)

DATE

RECEIVED

FORWARDED

OFFICER'S
INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

1. Acting Deputy to
the DCI for IC

2.

3.

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.